Using EMV cards to protect e-commerce transactions

Vorapranee Khu-smith and Chris J. Mitchell

Information Security Group, Royal Holloway, University of London,
Egham, Surrey, TW20 0EX, United Kingdom
{V.Khu-Smith, C.Mitchell}@rhul.ac.uk

Abstract. A growing number of payment transactions are now being made over the Internet. Although transactions are typically made over a secure channel provided using SSL or TLS, there remain some security risks. Meanwhile, EMV-compliant IC cards are being introduced to reduce fraud for conventional debit/credit transactions. In this paper, we propose a way of using EMV IC cards for secure remote payments, such as those made via the Internet, with the goal of providing protection against some of these residual risks. The scheme described in this paper is based on the EMV 2000 Integrated Circuit Card Specification for Payment Systems, which is first outlined. Threats to, and advantages and disadvantages of, the scheme are also examined.

Key Words: EMV cards; e-commerce security; payment protocol

1 Introduction

The Internet is now widely used for electronic commerce. Consumers typically make a payment with a debit/credit card and SSL/TLS is used to protect the transaction details against eavesdroppers. Although SSL/TLS has become a de facto standard means to secure an electronic transaction made over the Internet, it only provides security for the communications link between the consumer PC and the merchant server. As a result, there are a number of security risks in such use of SSL/TLS, as pointed out in [6]. One of these is the lack of client authentication and the associated lack of client non-repudiation. Even though SSL/TLS offers client-side authentication, it is optional and often bypassed. Consequently, it is not easy to verify if the client is the legitimate cardholder and there is no way to determine if the client actually has the card. A malicious user, who may have obtained a card number by some means, can then use it to make payments over the Internet at the expense of the legitimate cardholder.

Meanwhile, for transactions taking place at the Point of Sale (POS), a variety of frauds are possible against debit/credit card transactions. In recent years this has led the major card brands to develop an industry standard means of employing IC cards to replace the existing magnetic stripe cards, with a view to both reducing fraud and reducing the costs associated with online transaction authorisation at the POS. This collaboration between Europay, MasterCard and Visa resulted in the EMV card/terminal specifications, the latest version of which are known as EMV 2000 [1–4]. The EMV specifications standardise interactions between a debit/credit IC card and a terminal.

In an annex to Book 3 of EMV 2000 [3], the use of an EMV card and the Secure Electronic Transaction (SET) protocol [5] to conduct an e-commerce transaction is defined. However, SET (which provides security for an entire e-commerce transaction) has not been adopted to any significant extent—indeed, it is not clear if it will ever become widely used. Although the integration of EMV and SET removes some of the issues with SET, notably it simplifies user registration, there still remain large obstacles to its adoption.

As a result, in this paper we consider an alternative way in which the growing use of EMV IC cards can be used to enhance the security of e-commerce transactions. The goal is to design a scheme whereby EMV cards can be used to enhance e-commerce transaction security, and hence reduce fraud, whilst imposing minimal overheads on the involved parties. The paper begins with an overview of the EMV payment system. We subsequently propose the use of EMV cards for Internet electronic transaction processing. Threats to the proposed scheme are then analysed, and its advantages and disadvantages are considered.

2 An overview of EMV

In a debit/credit card payment system, there are four major parties, namely a client, a merchant, an acquiring bank and a card issuing bank. A client, i.e. the cardholder, makes a payment using a card issued by the card issuing bank (issuer) for something purchased from a merchant. The acquiring bank (acquirer) is the financial institution with which a merchant has a contractual arrangement for receiving (acquiring) card payments. The payment model is shown in Figure 1.

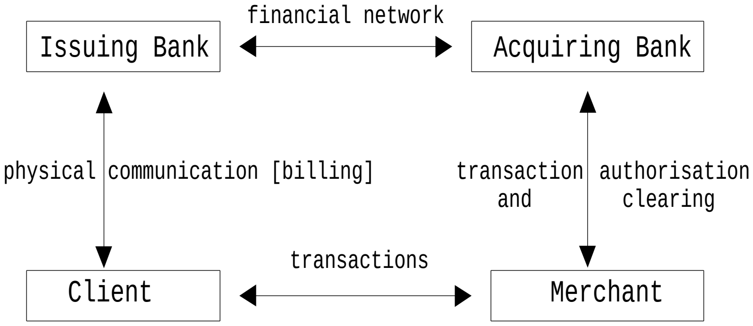

Fig. 1. Debit/credit card payment system model

The debit/credit card payment system is the model underlying the EMV system defined in EMV 2000 [1–4]. The EMV transaction process involves the following steps. Note that the order of the steps is not completely fixed; for example, cardholder verification can precede data authentication.

1. When the IC card is inserted, the terminal reads application data from the card and performs Terminal Risk Management. Terminal Risk Management provides positive issuer authorisation for high-value transactions and ensures that transactions initiated from IC cards go online periodically to prevent threats that might be undetectable in an offline environment.
2. The Data Authentication process enables the terminal to verify the authenticity of the card. There are two options for Data Authentication, namely Static and Dynamic Data Authentication. Not all EMV cards are capable of performing Dynamic Data Authentication.
3. After successful Data Authentication, the Process Restrictions are performed to determine the compatibility of the terminal and IC card applications.
4. Cardholder authenticity is verified by PIN entry. The PIN verification process can be either online to the issuer or offline to the card.
5. After successful Cardholder Authentication, the terminal performs Terminal Action Analysis, which is the first decision on whether the transaction should be approved offline, declined offline, or an online authorisation performed.
6. The IC card then performs Card Risk Management to protect the card issuer against fraud or excessive credit risk. Details of card risk management algorithms are specific to the issuer and are not specified by EMV.
7. The IC card performs Card Action Analysis to decide whether the transaction will be processed offline, or will need online authorisation. If the decision is offline processing, the transaction is processed immediately. If the transaction is to be processed online, Online Processing will be performed to ensure that the issuer can review and authorise or reject transactions that are outside acceptable limits of risk defined by the issuer, the payment system, or the acquirer. Issuers can also perform Script Processing, enabling command scripts to be sent to the card by the terminal to perform functions that may not necessarily be relevant to the current transaction but are important for the continued functioning of the card application.
8. The final process is Completion which ends the processing of a transaction.

In essence, the EMV scheme supports both cardholder authentication by PIN entry and IC card authentication through Static or Dynamic Data Authentication. Therefore, an unscrupulous user will find it hard to make a fraudulent transaction without possessing the actual card and the corresponding PIN.

We next focus on the security-related interactions between IC card and terminal. This is of particular interest here, since in the scheme proposed below the user PC plays the role of the merchant terminal and interacts with a merchant server across the Internet. The merchant server communicates with the acquirer, e.g. using the same interface as is currently used for merchant terminal-acquirer communications. An acquirer and an issuer typically communicate via a brand-specific network, which is outside the scope of this paper.

2.1 Card authentication

The EMV specifications allow card authentication to be either offline or online. The decision regarding whether to perform online authentication can be made by the IC card or the terminal at the time of the transaction.

Static data authentication (SDA). SDA involves the terminal verifying the integrity of static data signed by the card issuer and stored in the IC card. In this case the card does not need its own signature key pair.

SDA is supported by a two-level key management hierarchy. The top-level certification authority (CA) is the card scheme, e.g. Visa or Mastercard. This CA certifies the issuer public keys. The static data is signed using the appropriate issuer private key and stored in the card, along with the CA-signed certificate for the issuer public key. A terminal with a trusted copy of the CA public key can then verify the issuer public key certificate and hence can verify the signature on the static data, thereby verifying the IC card.

Dynamic data authentication (DDA). Like SDA, DDA is based on digital signatures, although in DDA the card has its own key pair. The terminal sends an Internal Authentication Command (IAC), including an unpredictable number, to the card. The card then digitally signs the IAC data. The terminal verifies the signature to authenticate the dynamic data and hence the card.

DDA is supported by a three-level key management hierarchy. The first and second level CAs are the card scheme and issuer respectively, and the card public key is certified by its issuer. In order to verify the signed data, the terminal needs to contain the top-level CA public key to verify the issuer public key certificate. The issuer public key is then used to verify the IC card public key certificate. The terminal can then verify the card signature.

2.2 Cardholder verification

The cardholder is verified using a PIN. The EMV Specifications require every EMV card to possess a method to limit the number of unsuccessful PIN tries.

PIN verification may occur offline to the IC card, or online to the card issuer (or a third party acting for the card issuer). For offline verification the PIN may be encrypted between the PIN pad and the IC card. A key pair assigned especially for PIN encryption or the key pair used in DDA can be used for encryption. In either case, the card public key is first retrieved by the PIN pad or a secure terminal component. The IC card also sends a random number to be concatenated with the entered PIN. The result is encrypted and sent back to the card. The card then decrypts the ciphertext, checks the random number and verifies whether the recovered PIN matches the one stored in the card.

2.3 Application cryptograms

Transaction message integrity and origin authentication are guaranteed by the use of Application Cryptograms (ACs), generated by the IC card and issuer using shared-secret-based Message Authentication Codes (MACs). There are four types of ACs, namely Transaction Certificates (TCs), Application Authentication Cryptograms (AACs), Authorisation Request Cryptogram (ARQCs) and Authorisation Response Cryptograms (ARPCs). If the transaction is approved offline, the card generates a TC. If the transaction is declined offline, then an AAC is generated. If the transaction needs to be approved online, the card generates an ARQC which will be sent to the issuer. The issuer then responses with an ARPC. As in the offline case, if the transaction is approved by the issuer, the card computes a TC; otherwise, an AAC is computed.

As mentioned above, ACs are cryptographically protected using a MAC. The issuer and card share a long term secret key MK_{AC} known as the card AC master key. This master key is used to generate an AC session key (SK_{AC}) which is used to compute the AC MACs. The session key SK_{AC} is computed as a function of MK_{AC} and diversification data R; the value R must be different for each session key generation to prevent replay attacks. Note also that, to avoid the issuer having to store the master key MK_{AC} for every card, each such master key is derived from an issuer master key MK_I. This key derivation takes as input the Primary Account Number (PAN) and the PAN sequence number.

3 Using EMV cards for e-commerce transactions

We now describe how an EMV-compliant IC card can be used to conduct remote transactions. The system architecture is described, as are the transaction processing procedures and how security services are provided.

3.1 System architecture

The e-commerce payment system we describe employs five main components: an EMV card, an IC card reader, the Cardholder System, the Merchant Server, and the Acquirer. We now examine each of these system components.

EMV card and IC card reader. The tasks of the EMV card are the same as those given in the EMV Specifications. The card is assumed to be a completely 'standard' DDA-capable EMV card — indeed, the scheme is designed so that existing EMV cards can be used to support e-commerce security without any modification. The EMV card interacts with a combination of system components, i.e. the card reader, the Cardholder System and the Merchant Server, just as it does with a merchant POS terminal.

The IC card reader, which can include a PIN pad, is required for interactions between the cardholder and the card, and between the card and the Cardholder System. Physical requirements for this device are similar to those in [1].

Cardholder System. The Cardholder System is the combination of hardware and software required to interact with the cardholder, the IC card, and the Merchant Server. The Cardholder System is assumed here to be a combination of a user PC and special purpose software which could, for example, be either a small program distributed with the IC card by the issuer or, to make system installation maximally transparent, a Web browser applet. The source of cardholder system software is not an issue we address here but it might be the card issuer, the card brand, or an associated party. The Cardholder System is jointly responsible, along with the IC card reader and the Merchant Server, for performing the tasks of the terminal defined in the EMV specification.

Merchant Server and Acquirer. The Merchant Server is the component that interacts with the Cardholder System to support electronic payments. The Merchant Server also interacts with the Acquirer. As specified above, the Merchant Server, the Cardholder System and the IC card reader collectively fulfill the role of the EMV merchant terminal. The Acquirer interacts with the issuer via the financial network to support transaction authorisation. To support SDA and DDA, the Merchant Server needs a trusted copy of the CA public key to enable it to verify issuer public key certificates.

3.2 Transaction processing procedures

In this section, we describe the processes necessary to complete a payment transaction. The protocol for using an EMV card for an e-commerce transaction is also described. The decision about which purchase to make are outside the scope of this paper — we simply assume that the cardholder and the merchant wish to perform a specified transaction.

The transaction flow is shown in Figure 2. In the protocol description, $X||Y$ denotes the concatenation of data items X and Y. Other terms are defined as they arise in the text below.

Card authentication and process restriction. A transaction begins after the cardholder has decided to make a purchase. The Merchant Server and the EMV card first perform SDA (step 1 in Figure 2). In this process, the Merchant first verifies the issuer public key certificate using its copy of the CA public key. The issuer signature on the Static Authentication Data (SAD), sent by the IC card, is then verified. Data communicated between the Merchant Server and the card are sent and received via the Cardholder System.

After successful SDA, the Merchant Server generates a random number, which is sent in the IAC, and constructs the purchase information (PI), which may contain a description of goods, the price, the date, and transaction id. The Merchant Server then sends $IAC||PI$ to the Cardholder System (step 2).

Upon receipt of the above message, the Cardholder System displays the purchase information to the cardholder and checks for the presence of an EMV card. It then forwards the IAC to the card (step 3). The IC card computes the signature $S_{IC}(DAD)$ and sends it to the Cardholder System along with the IC card's public key certificate Cert_{IC} (step 4), where DAD is the Dynamic Authentication Data containing the random number sent in the IAC. In step 5, the Cardholder System sends $S_{IC}(DAD)||\mathrm{Cert}_{IC}$, to the Merchant Server. Since the issuer public key is used and verified in the SDA process, the Merchant Server now only needs to verify the card certificate and then the signature $S_{IC}(DAD)$.

After successful card authentication, Process Restriction (step 6) is performed. Data Authentication and Process Restriction take place between Mer-

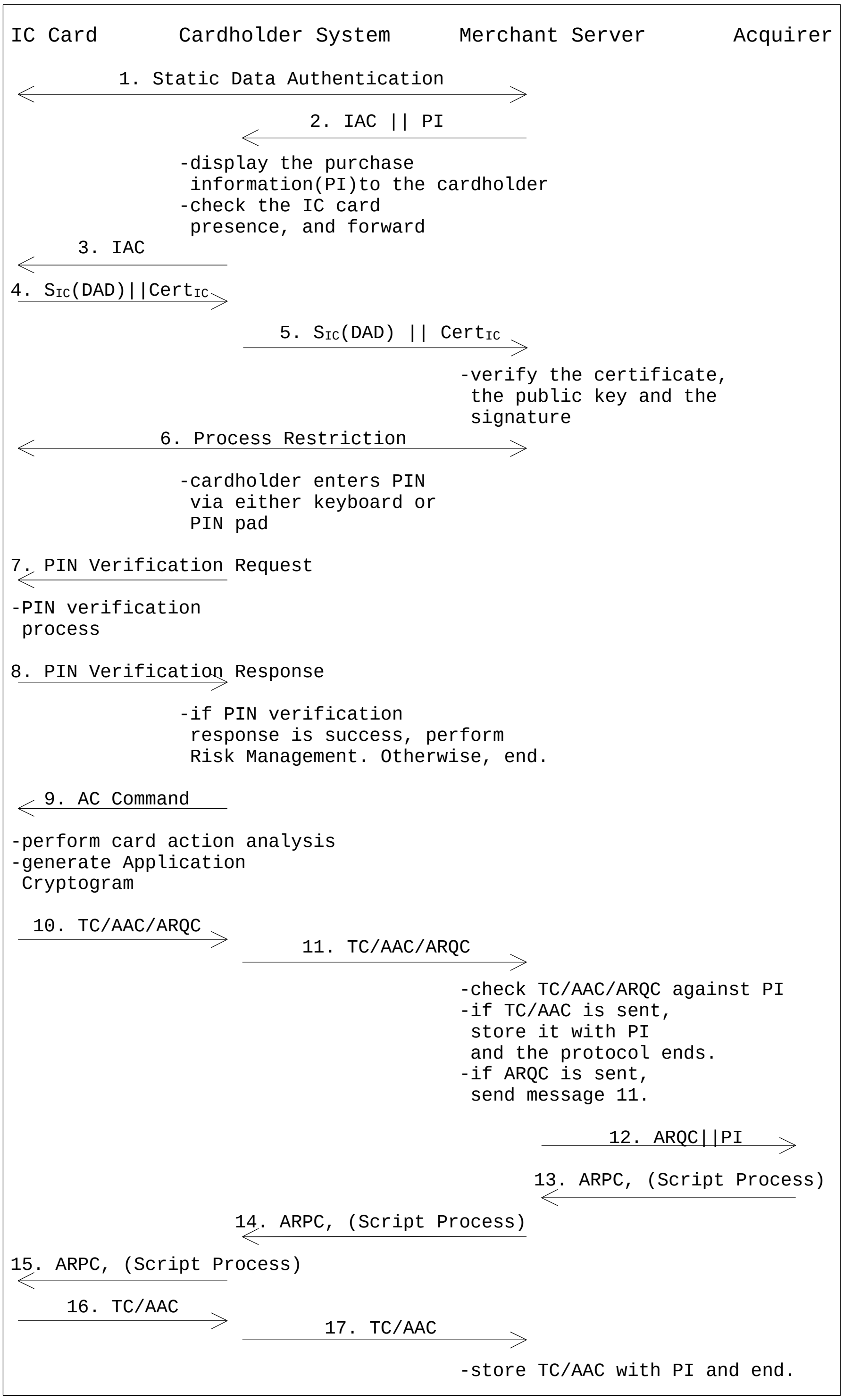
IC Card
Cardholder System
Merchant Server
Acquirer
1. Static Data Authentication
2. IAC || PI
-display the purchase information(PI)to the cardholder
-check the IC card presence, and forward
3. IAC
4. S_{IC}(DAD)||Cert_{IC}
5. S_{IC}(DAD) || Cert_{IC}
-verify the certificate, the public key and the signature
6. Process Restriction
-cardholder enters PIN via either keyboard or PIN pad
7. PIN Verification Request
-PIN verification process
8. PIN Verification Response
-if PIN verification response is success, perform Risk Management. Otherwise, end.
9. AC Command
-perform card action analysis
-generate Application Cryptogram
10. TC/AAC/ARQC
11. TC/AAC/ARQC
-check TC/AAC/ARQC against PI
-if TC/AAC is sent, store it with PI and the protocol ends.
-if ARQC is sent, send message 11.
12. ARQC||PI
13. ARPC, (Script Process)
14. ARPC, (Script Process)
15. ARPC, (Script Process)
16. TC/AAC
17. TC/AAC
-store TC/AAC with PI and end.

Fig. 2. Transaction flow for remote EMV

chant Server and card, and the Cardholder System simply forwards messages. Note that these processes remain unchanged from the EMV specification.

Cardholder verification. The Cardholder System next requests the cardholder to enter the PIN; PIN verification can take place online or offline. To perform offline verification, the Cardholder System sends a PIN Verification Request message to the IC card (step 7). The PIN does not need to be encrypted, since the environment is under cardholder control. On receipt of the PIN Verification Request, the EMV card returns a PIN Verification Response message (step 8) which indicates whether PIN verification is successful. If so, the Cardholder System performs Terminal Risk Management; otherwise, the protocol ends.

Terminal risk management and action analysis. After successful cardholder verification, the Cardholder System performs Terminal Risk Management and Terminal Action Analysis. These two processes are as in the EMV specification. The Cardholder System then generates and sends an AC Command to the EMV card (step 9).

Card action analysis. The IC card first performs its own risk management and then executes the Card Action Analysis to determine whether the transaction is to be approved offline, rejected offline, or processed online. In step 10, an AC will be generated by the IC card and sent to the Cardholder System. The Cardholder System in turn forwards it to the Merchant Server (step 11) where the AC will be checked against the PI.

Offline approval. If the transaction is approved offline, the card generates and sends the TC to the Cardholder System, from where it is forwarded to the Merchant Server (steps 10/11). The TC will be held with the PI and acts analogously to the receipt in a conventional payment system. The Merchant Server can later send a batch of TCs, with the corresponding PIs, to the Acquirer. The issuer will verify the MAC in the TC and compare the information in the TC with that in the PI. If they match, the payment is accepted and processed.

Offline decline. If the transaction is declined offline, the IC card generates an AAC which is sent to the Cardholder System where it will be forwarded to the Merchant Server (steps 10/11). The merchant can store the AAC with the PI for card management purposes, and the transaction now ends.

Online processing. If the IC card decides that online authorisation is needed, it generates an ARQC which is forwarded to the Merchant Server via the Cardholder System (steps 10/11). The Merchant Server then sends the ARQC with the PI to the Acquirer and thence to the issuer (step 12). The issuer responds to the ARQC with an ARPC (step 13). The Script Processing may also now be performed by the issuer, to send command scripts to the IC card (steps 14/15). The transaction will be accepted or declined according to the ARPC. If it is accepted, the IC card generates a TC (step 16) and the process previously described under offline approval is performed. Similarly, if the transaction is declined, the IC card generates an AAC (step 16). The TC or AAC is then forwarded to the Merchant Server (step 17) and the transaction processing ends.

3.3 Security services

We now describe how the desired security services are provided.

Authentication. Cardholder and IC card authentication are provided in the same way as in 'standard' EMV. Cardholder authentication is based on knowledge of a PIN. IC card authentication uses SDA and DDA. Merchant Server authentication, however, is not provided in the protocol.

Confidentiality and integrity. Although the entered PIN is not encrypted, its confidentiality and integrity are protected since it never leaves the environment over which the cardholder has control. AC integrity is guaranteed by the use of MACs, as in the EMV specifications. Nevertheless, AC confidentiality is not provided by the protocol. Unlike in a conventional EMV environment, it is transmitted over an unprotected link, i.e. the Internet. Therefore, it is possible for an eavesdropper to learn the card details contained in the ACs.

Non-repudiation. A measure of Cardholder non-repudiation is provided by the TC. The existence of a valid TC provides evidence that the cardholder authentication process has taken place, and hence the cardholder has consented to the transaction by entering his/her PIN. By contrast, merchant non-repudiation is not provided, although the value of such a service is unclear.

4 Threat analysis

In the protocol, there are five locations where the transaction data is at risk. These are the Cardholder System, the card reader, the link between the two, the Internet link between Cardholder System and Merchant Server, and the Merchant Server. Threats to the Merchant Server-Acquirer link are outside the scope of this paper, since such threats apply equally to conventional use of an EMV card, and we only consider here threats introduced by 'remote EMV'. Also, since physical access to the Cardholder System, the card reader, and their link is limited to the cardholder, the cardholder is the only threat to them.

Therefore we divide our threat analysis into three parts, namely threats to the cardholder environment, threats on the Internet link, and threats at the Merchant Server. In each case, the possible types of transaction data which may be at risk are considered, along with the entities who may pose a threat. There are six types of transaction data that need to be examined, namely the Static Authentication Data (SAD), PI, IAC, $S_{IC}(DAD)$, PIN, and four ACs. Note, however, that integrity threats to $S_{IC}(DAD)$ and the four ACs are minimal since they are cryptographically protected using 'standard' EMV techniques. We thus focus most of our attention on the SAD, PI, IAC, and PIN.

Threats at the cardholder system. We refer to the combination of Cardholder System, card reader, and link between the two, as the cardholder environment. The SAD, PI, IAC, $S_{IC}(DAD)$, PIN, and four ACs pass through this environment. However, cardholder threats to the SAD, IAC, $S_{IC}(DAD)$, and PIN are not serious since the cardholder has the card and knows the PIN.

A malicious cardholder can modify the PI to make the Cardholder System send a smaller transaction value to the card than specified by the Merchant

Server. However, the fraud will be detected as soon as the AC arrives at the Merchant Server. As a result, modifying the PI yields little to the cardholder. More seriously, because the Merchant Server does not have the MAC key necessary to verify the ACs, the Merchant Server cannot determine if the ACs received are authentic. Modifying the ARQC and the ARPC will yield no gain since they are sent online to the issuer, and altering the AAC is also unattractive for the cardholder because it yields nothing financially. However, an unscrupulous cardholder can modify or replace an offline-approved TC sent from the IC card, thereby causing the payment capture to fail at a later stage.

However, this risk also exists in the conventional EMV environment. Special equipment could be used to interfere with the communications between the POS terminal and the IC card. As in our scheme, the equipment could replace or modify the TC so that the MAC becomes invalid. A possible way to address this threat is to delay DDA until the TC is generated, and then include the TC in the DAD signed by the card. The Merchant Server can verify the card public key and signature, using the issuer public key, thereby guaranteeing the authenticity of the TC. Including the TC in the DAD should not be a problem in the future, since such a process is supported by the latest version of the EMV specifications (see Section 6.6 of [2]).

Threats to the Internet link. The transaction data at risk on the Internet link are the SAD, IAC, PI, and the four ACs. The main threat here is a third party eavesdropper (passive or active). From a third party point of view, modifying the four types of transaction data is possible but also detectable, and there is little possibility for financial gain. The only benefit may be to deny service, a threat that always exists when using a public network.

A threat does arise from the way SAD is authenticated. Only the issuer signature on the static data is verified. Therefore, it is possible for an attacker to replay the SAD and pass the SDA process. Nevertheless, if DDA is performed, the attacker will not be able to generate a valid $S_{IC}(DAD)$ and hence cannot complete the transaction process.

Reading the four Cryptograms can provide an attacker with the card/account details. However, if the proposed protocol is in use, an EMV card and the corresponding PIN are required to complete a transaction. As a result, knowing only the account/card number is not so useful. If confidentiality of the ACs is a concern, a way to reduce the threat is to employ a secure channel such as TLS or HTTPS to protect the Internet link. This is a cheap, user-transparent and simple solution, since the technology is already widely available (and widely used). Use of TLS can also provide other security services such as additional integrity checks and Merchant Server authentication.

Threats at the Merchant Server. The transaction data available at the Merchant Server are the *SAD*, *IAC*, *PI*, and the ACs. The Merchant Server is either the legitimate recipient or the generator of the four types of data. There is thus no serious threat to data confidentiality. There is also no obvious financial gain for the merchant from breaching data integrity. The ARQC and the ARPC will be sent online to the Issuer, and the TC and the PI will also be checked by the issuer. If any modification is detected, the payment capture or authorisation process will fail. It is also clear that there is no point in modifying the SAD or the IAC since doing so will simply interrupt the transaction process.

5 Advantages and disadvantages

Using EMV cards to make a remote payment may compromise certain EMV security elements. A POS system has the advantage of face-to-face interactions as well as use of a tamper-resistant POS terminal. By contrast, Internet transactions involve no face-to-face interactions, and the terminal, here a combination of card reader, Cardholder System and Merchant Server, is clearly not tamper-resistant. Indeed, certain data which would be sent via internal communications in an EMV POS terminal, are sent via the Internet in the proposed scheme.

The proposed protocol enhances the security of existing Internet payment methods, typically relying on SSL/TLS for transaction security. There are known security risks with such an approach, including lack of cardholder authentication [6]. Our scheme provides cardholder authentication by using EMV PIN verification. The PIN is also associated with the IC card such that without the correct PIN the card will not work and hence no transaction can be made.

A major advantage of the scheme is that it uses existing technologies. This include the EMV PKI established by the card brands and the issuers, and the EMV cards themselves. Moreover, the scheme reduces the online authorisation overhead because the IC card can make some decisions offline. Using an IC card remotely does requires special software (e.g. an applet) to be installed in the cardholder PC. An IC card reader is also needed. Nevertheless, use of the proposed scheme is 'light' compared to the SET initialisation process.

The protocol does rely on Cardholder System integrity, since the Cardholder System could be modified by a malicious cardholder to send a bogus TC or by an unscrupulous merchant to display different payment information to the cardholder from that sent to the IC card. Another weakness of the proposed protocol may be that confidentiality of the card details is not provided; the Cryptograms are transmitted over the Internet and hence may be intercepted. However, as described above, a secure channel can be used in combination with the protocol to protect the transaction data en route.

6 Conclusions and directions for future research

In this paper, we have proposed a way to use an EMV-compliant IC card for e-commerce transactions. In the scheme, a user card reader and PC (the Cardholder System) together with the Merchant Server collectively take the role of the EMV Merchant Terminal. Most of the transaction procedures are similar to those in the EMV specification. Although some of the EMV security requirements are compromised, the proposed scheme can be seen as a step towards enhancing the existing SSL/TLS enabled electronic transaction processing.

The most closely related work is probably the scheme described in an annex of [3]. This scheme combines SET with EMV-compliant IC cards to conduct Internet transactions. However, as discussed in the Introduction, there remain serious obstacles to the use of SET.

GeldKarte [7] is an electronic cash card developed by the German banking industry. GeldKarte applications have also been extended to Internet uses, allowing the cardholder to use the value in the card to buy things from the Internet as well as to enhance the security of Internet transactions. However GeldKarte is clearly different from the proposed protocol since it is an electronic cash scheme.

To reduce the trust required in the Cardholder System, and prevent any attacks by malicious cardholders, a trusted card reader with a simple user interface such as a PIN pad and small display could be used. It is interesting to consider to what degree the risks of a remote EMV transaction could be reduced by using such a trusted card reader, and this is a possible topic for future research. How payment schemes might best be designed to use such a trusted card reader is also a possible future research topic. Finally, a further possible research area relates to mobile-commerce (m-commerce). It would be interesting to see how the proposed protocol could enhance the security of m-commerce by using a mobile phone as both the IC card reader and the Cardholder System.

References

1. EMV. *EMV 2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 1: Application Independent IC Card to Terminal Interface Requirements.* EMVCo, 2000.
2. EMV. *EMV 2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 2: Security and Key Management.* EMVCo, 2000.
3. EMV. *EMV 2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 3: Application Specification.* EMVCo, 2000.
4. EMV. *EMV 2000 Integrated Circuit Card Specification for Payment Systems Version 4.0 — Book 4: CardHolder, Attendant, and Acquirer Interface Requirements.* EMVCo, 2000.
5. SETCo. *Secure Electronic Transaction Specification — Books 1–4.* SETCo, 1997.
6. L. D. Stein. *Web Security: A step-by-step reference guide.* Addison Wesley, 1999.
7. R. Keller, G. Zavagli, J. Hartmann, F. Williams. *Mobile Electronic Commerce: Research investigation into loading and paymnet functionality in wireless wallets.* available at http://citeseer.nj.nec.com/cs, 1998.