Royal HOLLOWAY SERIES 2012

# A More Ubiquitous Card Present Payment Scheme

*The ARJA system is a proposed payment scheme that uses near-field communications and contactless cards to replace point-of-sale terminals and support mobile device payments. Find out how ARJA could lead to more secure transactions.*

**BY ALBERT ATTARD AND ADRIAN LEUNG**

TechTarget

Royal Holloway University of London

# Payment over the Internet

PAYMENT OVER THE INTERNET

A WAY FORWARD

**HERE WE LOOK** at security advances made by the payment industry, focusing on credit cards. After reviewing existing Internet payment schemes, the authors propose a new payment scheme that makes use of near-field communication (NFC) and contactless cards. The scheme replaces point-of-sale (PoS) terminals with two applications, one running on a mobile device and the other running on an application server. It is akin to having a portable PoS terminal in the customer's pocket which can be used anytime and anywhere.

## PAYMENT OVER THE INTERNET

How payment is made over the internet greatly depends on where goods, products or services are bought from as different methods are available. Most methods involve entering credit or debit card details into the website. From there the payment is processed, which in turn leads to a debit from the card account. This has been the predominant method of making payments over the Internet since its conception. Such transactions are protected by the SSL protocol, which provides a secure communicating channel between the customer's Web browser and the merchant's website. SSL is not a payment protocol and does not provide security features such as payment confirmation, non-repudiation or protection of card details at the merchant's end.

## PAYMENT USING A CREDIT CARD

Until recently, in shops the credit card was swiped at the PoS terminal after which the customer signed the chit, authorising the purchase. But this is now history, at least in many countries. The payment industry moved away from the magnetic stripe cards and embarked on a new area of payments using smart cards, also known as "Chip and PIN". The latter provides a higher degree of security when compared with the magnetic swipe card. The payment is carried out using standard protocols which cater for payment specific needs such as ensuring that the credit card has enough funds to cover the transaction.

Here we briefly survey the security advances made by the payment industry in the area of credit cards. We then cover existing Internet payment schemes in a little detail before proposing a new payment scheme that makes use of additional features found in the latest mobile technology.

## HOW DID CREDIT CARDS EVOLVE AND WHY?

The credit card era started in earnest in 1950 when Frank X. McNamara invented the Diners Club card. Short of money during an important dinner the previous year, McNamara came up with the idea of issuing credit cards to avoid such an embarrassment. The credit card not only acted as a method of payment but also as a status symbol, distinguishing the cardholder from others.

Banks soon took up the idea. The payment process was very simple. Using a "zip-zap" manual swipe machine, the cashier made a copy of the credit card embossed on a paper document provided by the bank. Together with the credit card details, this document also included the transaction amount together with the customer's signature. The "zip-zap" manual swipe machine simply copies the information from the credit card to a paper document. This is then signed by the customer and the cashier verifies the signature together with the authenticity of the credit card. The process is called authentication. The cashier authenticates the customer by comparing the signatures found on the credit card and the one just produced. Furthermore, the cashier authenticates the credit card to ensure that it is valid—by observing the hologram, for example. By signing the document, the customer is also authorising the payment. Finally, the merchant takes this document to the bank and receives the money if the credit card contains enough funds to honour the transaction. However, this procedure has a high level of fraud as it has many security gaps. For example, the method does not ensure that the customer has enough funds to cover the required payment.

***The credit card not only acted as a method of payment but also as a status symbol, distinguising the cardholder from others.***

**TABLE 1.**
Comparison of the authentication, authorisation and transfer of funds between the different types of card

| CREDIT CARD | AUTHENTICATION & AUTHORISATION | TRANSFER OF FUNDS |
|---|---|---|
| "Zip-zap" manual swipe | Manual | Manual |
| Magnetic stripe | Manual | Automatic |
| Chip and PIN | Automatic | Automatic |

The **magnetic stripe card** was introduced to address some of the security gaps found in the previous version. These cards include a magnetic stripe on the reverse which allows a PoS terminal to read the credit card details electronically. This enabled PoS terminals to connect to the bank, verify the validity of the card and authorise payments automatically. Despite the new security mechanism employed, these credit cards can be easily cloned and are still subject to various threats.

The increasingly high financial losses due to the security weaknesses found in magnetic stripe cards gave birth to the EMV protocol. It makes use of smart cards, instead of magnetic swipe cards. These are infeasible to clone or compromise because of their tamper-resistant built-in chips. In the UK, the EMV protocol was branded as "Chip and PIN". EMV is an international standard that defines the communication between the smart card, the PoS terminal and the card issuer for authenticating and authorising payments.

**TABLE 1** compares the authentication, authorisation and transfer of funds between the different types of card.

EMV provides better authentication and authorisation of payments than its predecessor. It uses a PIN and cryptographic mechanisms to authenticate the customer and credit card with the bank and to authorise the payment. It does not rely on signature and other checks that are carried out less accurately by the cashier. The EMV standard removed the human factor, known to be very vulnerable to several fraud attacks, from the authentication process. This change in technology led to a drastic reduction in fraud through electronic payments. In the UK alone, losses in the high street were reduced by 67% from £218.8m in 2004 to £72.1m in 2009.

**Contactless credit cards** form a new breed of credit card built on top of smart card technology. These cards do not introduce new security features but improve card accessibility. They enable payments by simply bringing the credit card into proximity to the PoS terminal. The two components establish a communication channel over the air and facilitate the payment using NFC without the need to be physically connected. For small amounts, such as payment for a coffee, the customer is not requested to provide the PIN. This shortens the payment time and therefore queue lengths at the cashier, but once a pre-set number of payments have been made, the customer will be forced to provide the PIN again for security reasons. This limits the amount of theft before the PIN is required should the card be used without the card owner's knowledge and consent.

The protocol proposed in this article makes use of the EMV protocol and contactless credit cards. It replaces the PoS terminal with two applications, one running on a mobile device and the other running on an application server. This is like having a portable PoS terminal in the customer's pocket which can be used anytime and anywhere.

PAYMENT OVER THE INTERNET

A WAY FORWARD

## DETAILS OF PAYING USING CREDIT CARDS ON THE INTERNET

When a customer is ready to pay for goods or services from the Internet, he or she proceeds to the payment web-page and provides the required credit card details, usually including the address of the card holder. The merchant processes these and verifies that the customer has enough funds to make the payment before dispatching the goods and billing the customer via the credit card company. The merchant or anyone else in possession of these same credit card details can clearly perform another payment over the Internet without owning or holding the credit card. This is because many Internet payments schemes perform what is referred to as a **card-not-present** transaction.

In a card-not-present transaction the credit card is not authenticated during the payment process. Only the numbers on the card are required to perform the payment. This is very similar to the first two versions of the credit cards (Zip-Zap and Magnetic Stripe), where the card was easily cloned. But here it is even simpler since copying of the card details is enough to purchase goods in a card-not-present transaction. On numerous occasions children have stolen money from their parents by copying their parents' credit card details and purchasing goods online. This has become worse with the advent of so many online service providers. Their services (for example, website access or content download of music) are consumed online without the need for a delivery address, thus making it harder to trace the criminal. This is only partly mitigated by service providers generally requiring users to register and login with a username and password.

PAYMENT OVER THE INTERNET

A WAY FORWARD

## A COMPARISON WITH PAYMENTS MADE AT A BRICKS-AND-MORTAR STORE

In order to make a smart card payment at a bricks and mortar store a customer will need to be in possession of a valid credit card and know the corresponding PIN for the credit card. Both are required for the payment system (such as the bank or credit card company) to authenticate the transaction. This is commonly referred to as *two factor authentication* as the authentication process requires two things of a different nature: here they are something you *have* (the credit card) and something you *know* (the PIN). Presenting just the credit card details will buy you nothing as only production of the card itself together with use of the correct PIN will work at the store. Another common authentication factor is something you *are*, such as a biometric or signature. The magnetic swipe card too makes use of two factor authentication: something you have (the credit card) and something you are (the signature).

This process is referred to as a **card-present transaction**. In contrast to the card-not-present transactions, the chip card is authenticated by the bank using cryptographic mechanisms. This ensures that both the credit card and the PIN are valid.

Few Internet payments schemes use card-present transactions where the credit card is authenticated as part of the process. As mentioned before, the credit card details usually required can easily be “cloned” as they are only text, which is no better than the “zip-zap” magnetic stripe era. Indeed, some believe that the magnetic stripe cards and signatures are more secure than such Internet payments even when protected by a requirement for login to the merchant’s website. The username/password pair is subject to several attacks and vulnerable to many threats whereas signatures are regarded as harder to compromise. The former uses only one factor authentication, namely something you know (the username/password), whereas the swipe card uses two factor authentication. ■

**To pay in a physical store a customer needs to:**

- **Be in possession of a valid smart credit card**
- **Know the corresponding PIN for the credit card**

**OR**

- **Be in possession of a valid swipe card**
- **Be able to produce the correct signature.**

**This is called *two-factor authentication.***

# A Way Forward

**WE ARE PROPOSING** a novel payment protocol, named ARJA, that makes use of the security provided by the EMV standard in mobile devices with NFC technology. ARJA means "air" in Maltese, which is synonymous with the method of communication—contactless. The proposed protocol enables card-present transactions for Internet payments with the same level of security found when purchasing from a bricks and mortar store.

The concept is very simple. The mobile phone acts as a catalyst between the customer and the payment system, such as the bank. Instead of entering credit card details to a website, the customer uses his or her mobile phone as a card reader for a contactless credit card in order to authorise payments. The protocol, described in the following steps, just requires also that the merchant be enrolled on the ARJA payment scheme so that it can accept ARJA payments.

The steps listed below provide an overview of the ARJA protocol.

1. **The customer selects** the ARJA payment scheme as the payment method for his contactless credit card.

2. **The merchant generates** a unique code that identifies this transaction and registers the transaction with the ARJA Server Application, which is a trusted application hosted by banks or payment gateways (not the merchant).

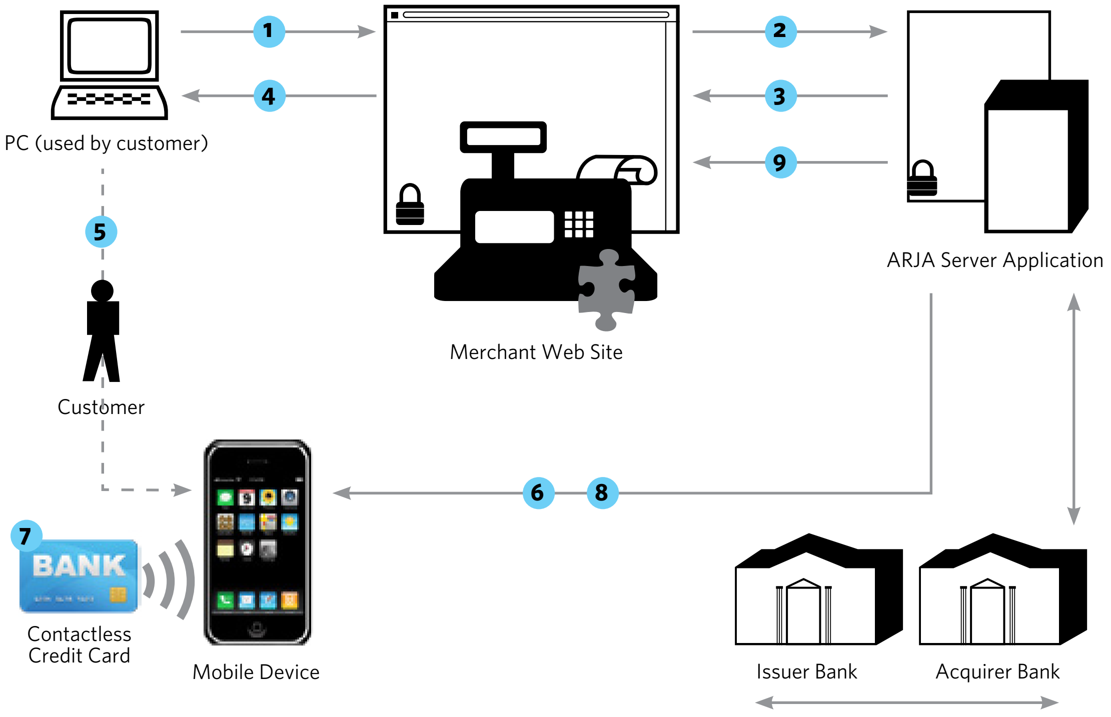
3. **The ARJA Server Application generates** a token which is bound to this transaction and returns this to the merchant.

4. **The merchant forwards** this token to the customer, which is displayed on his browser.

5. **If not done automatically**, the customer enters this code into the ARJA Mobile Application on his phone. This application will have been previously downloaded securely from the same organisation as hosts the ARJA Server Application.

6. **The ARJA Mobile Application downloads** the transaction details from the ARJA Server Application and displays them on the mobile screen. These details include the transaction amount and the merchant name together with other relevant information. This step provides the customer with a trustworthy display showing how much he or she is paying and to whom. It is an improvement over the PoS terminals found at physical stores which are subject to man-in-the-middle attacks.

**FIGURE 1.**
Overview of ARJA protocol



1 Checkout
2 Register Payment Request
3 Payment Request Reference
4 Payment Request Reference
5 Payment Request Reference
6 Download the Merchant name and the payment amount
7 Confirms Payment and Provides PIN
8 EMV
9 Transaction Certificate

PAYMENT OVER THE INTERNET

A WAY FORWARD

7. **Next, the customer places** the contactless credit card near the NFC-enabled mobile phone, using it as a card reader, and enters the PIN to authorise the payment or simply cancels the transaction.

8. **The ARJA Mobile Application transmits** this information securely to the ARJA Server Application. If the transaction is approved, the ARJA Server forwards the details to the bank. The ARJA Server also notifies the merchant of the transaction outcome and provides a receipt as necessary to the customer.

This is very similar to what happens at a PoS terminal but executes the EMV protocol through a new path. Instead of using a fixed PoS terminal installed at a merchant's shop, it enables the mobile device, with NFC support, to become a portable PoS terminal or card reader. Furthermore, the same mobile device can be used to purchase articles or services from various merchants and may be used by different customers. The proposed

## ARJA OVERVIEW

**The customer selects ARJA for paying.**

- **The merchant sends the transaction details and a unique transaction code to the payment gateway's ARJA Server Application.**
- **The ARJA Server Application generates a token (referred to payment request reference) and returns this to the Merchant.**
- **The transaction token is also sent to the customer... and entered into his ARJA Mobile Application.**
- **The trusted ARJA Mobile Application downloads the transaction details from the ARJA Server and displays them on the mobile screen.**
- **The customer uses his mobile phone with NFC technology as a card reader and enters the PIN to authorise payment (or cancels it). This approval (or otherwise) is then transmitted to the ARJA server.**

**Finally, the ARJA Server forwards:**

- **the transaction details to the bank for payment**
- **the transaction confirmation (or cancellation) to the merchant**
- **a receipt to the customer.**

solution removes the affinity between the merchant and the PoS terminal. The entered PIN is not remembered by the ARJA Mobile Application, and the customer has to provide this for every transaction.

## WHAT ARE THE ADVANTAGES OF THE ARJA PROTOCOL?

The ARJA Protocol has a number of advantages, such as the following:

**No username and password.** No registration is required by the customer on the website nor passwords remembered in order to use this protocol. This mitigates the risks associated with the username and password access control mechanism used widely throughout the Internet for services. The customer is authenticated by the card issuer using the credit card and its PIN.

### ADVANTAGES OF ARJA

1. **No username and password for the website.**
2. **Credit card details are not disclosed to merchant.**
3. **Customer anonymity if desired.**
4. **Only card-present transactions occur.**
5. **Purchase details are not disclosed to bank.**
6. **Trustworthiness of displayed transaction information.**

**Credit card details are not disclosed.** The credit card details are never entered into any website nor stored by the merchant during the payment process, nor seen by either the ARJA Server Application or the ARJA Mobile Application. The customer simply puts the contactless credit card near the mobile device and the payment details are securely transferred to the bank in an encrypted packet for processing. The merchant is never in contact with such information. This mitigates the risks associated with card detail theft from third parties such as merchants and can provide anonymity to the customer.

**Card-present transactions.** The credit card performs an EMV card-present transaction over the Internet. This mitigates the risks associated with card-not-present transactions as both the credit card and the PIN are required during the payment process. The credit card is authenticated on-line which also mitigates attacks related to off-line card authentication.

**Purchase details are not disclosed.** The customer does not share the purchase details with any other entity but the merchant. This promotes privacy as the ARJA Server Application, and the banks do not receive such information.

**Trustworthiness.** The ARJA Mobile Application provides a trustworthy display as this application is digitally signed by the ARJA provider. The customer paying with this protocol has the ability to use the signature to verify that the ARJA Mobile Application was not compromised and therefore that the payment was handled in a secure manner. Thus the information displayed by this application is reliable: correct and not compromised. The customer can ascertain that the merchant indicated by the ARJA Mobile Application is indeed the recipient of the money indicated by the same application.

PAYMENT OVER THE INTERNET

A WAY FORWARD

## CONCLUSION

A significant card-present protocol has been described for authenticating payments over the Internet using the NFC technology of current mobile phones. Two important security features that this protocol provides are customer anonymity and trustworthiness of transaction details. The customer does not need to create accounts with the merchant and credit card details are never saved by the protocol, enabling him to remain anonymous. The customer can also ascertain that the correct payment will go to the right merchant because of the secure connection between him and the card provider. These properties protect the customer while purchasing over the Internet and will lead to much lower levels of fraud. In the near future one should expect card-not-present transactions to become almost only of historic interest. ■

## ABOUT THE AUTHORS:

**Albert Attard** is a chief technical architect currently employed with a betting company. He leads a team of developers and manages numerous highly scalable enterprise applications.

**Adrian Leung** works in enterprise risk for a major management consultancy and is a project supervisor for Royal Holloway's MSc programme in information security.