Journal of Information Security and Applications 40 (2018) 103–110

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

A comparative study of card-not-present e-commerce architectures with card schemes: What about privacy?

A. Plateaux, P. Lacharme, S. Vernois, V. Coquet, C. Rosenberger*

Normandie Univ, UNICAEN, ENSICAEN, CNRS, GREYC, Caen 14000, France

ARTICLE INFO

Article history:

ABSTRACT

Internet is increasingly used for card-not-present e-commerce architectures. Several protocols, such as 3D-Secure, have been proposed in the literature by card schemes or academics. Even if some of them are deployed in real life, these solutions are not perfect considering data security and user's privacy. In this paper, we present a comparative study of existing solutions for card-not-present e-commerce solutions. We consider the main security and privacy trends of e-payment in order to make an objective comparison of existing solutions. This comparative study illustrates the need to consider privacy in deployed e-commerce architectures. This has never been more urgent with the recent release of the new specifications of 3D-secure.

1. Introduction

E-commerce has developed significantly in recent years, with 1.4 billion of online shoppers are counted in the World in 2016 [1] for a total amount of transactions near 2.7 billion dollars. In 2016, the fraud amount in electronic payments increases with the same regularity. Today, it becomes an important preoccupation for both financial institutions and users, and a problem of trust between the different actors [2]. Despite the fact that personal data is exchanged with e-commerce websites during an online payment, the banking industry mainly focuses on identity spoofing and user authentication. The electronic transaction security should not be strengthened at the expense of privacy protection, and a consumer centric privacy system should ensure data privacy with a possible control by users over their personal information [3].

Four actors are necessarily involved in electronic payments during a *card-not-present transaction*. The *client* (also called the cardholder) browses on the website of the merchant, called *service provider* (or *SP*), to buy an online service. These two actors have a payment provider, respectively called the issuer bank and the acquirer bank. Nevertheless, in most online payment schemes, other actors are involved. They are generally employed as trusted third party, with various roles. For example, it can be an interoperability system, such as in 3D-Secure, or an identity provider operated by the banks themselves, such as the BankID system [4]. In addition, an authentication system for payment providers is required for fraud resistance but is generally not described in these protocols. Finally, alternative payment systems such as the three-party model PayPal are out-of-scope of this paper. Indeed, we focus in this paper on e-commerce architectures involving banks (representing a large proportion of e-payments).

During an online purchase (card-not-present transaction), the client sends various banking information such as the PAN (Primary Account Number), the expiry date of the card and the secure cryptogram *CVX*2 (Card Verification Value/Code). This online service generally uses a secure connection between the client and the SP website, using a protocol such as SSL/TLS, ensuring the confidentiality and the integrity of the transaction on the Internet. But, in the same time, neither the client's authentication, nor the confidentiality of the data, on the merchant and bank parts, is granted. In basic systems, the client authentication is realized with the knowledge of these banking information (particularly the CVX2), whereas with *advanced* systems, such as 3D-secure, the authentication is strengthened by an additional data (in complement to banking information), as described below. This additional data is generally an OTP sent by SMS on the mobile device of the user, even if the NIST has recently warned against this system for payments [5].

Historically, many architectures have been defined for client authentication during a card-not-present transaction such as SET (Secure Electronic Transactions [6]). SET is quickly replaced by 3D-secure, that is widely used for many transactions [7]. In addition, alternative protocols have been proposed in the academic literature [8–10], in order to strengthen the lack of privacy in 3D-secure. Nevertheless, there is no real comparison between these protocols

* Corresponding author.
E-mail address: christophe.rosenberger@ensicaen.fr (C. Rosenberger).

https://doi.org/10.1016/j.jisa.2018.01.007
2214-2126/

in term of architecture, security and privacy objectives. Finally, two new specifications have been recently published, with a tokenization approach [11] and a new version of 3D-secure (v 2.0) [12–15]. These specification are described with a special target on mobile devices, providing a new architecture for these electronic payments, where user's privacy has been totally abandoned in favor to fraud detection by the banks. Another EMV-compliant payment system using tokenization, where the security is based on the secure element of a mobile has also been recently proposed in [16].

The objective of this paper is to make a comparative study of existing architectures for e-commerce. As many main papers in the literature [17–19], we focus on security trends an architecture must fulfill within this context. We also consider privacy trends to analyze the benefit of the architecture proposed in the state of the art, we think this issue is becoming more and more important nowadays as big data is operational in many applications. The machine learning capabilities are able, for example, to identify an individual by analyzing its e-commerce behavior. Finally, we also propose a comparative study on the new specification of 3D-secure with a particular attention on electronic payment with mobile platforms.

Section 2 presents the context of online payments and defines the requirements for user's privacy and data security. Existing card payment architectures in the literature are detailed in Section 3. Section 4 presents a comparative study of architectures in the state of the art by considering security and privacy trends. Finally, conclusions and perspectives are given in Section 5.

2. Security and privacy protection requirements

This section establishes a set of security and privacy requirements for an authentication protocol for online payments (with a usability requirement), complementing previous works presented in [10,20,21]. Personal data involved in online payments should be divided in several parts (three parts in the present paper), because these data are shared between several entities, that have no operational requirements for access to all these data (except maybe for fraud detection):

1. The identity information are the data linked to the client's identity, such as a name, a home phone (or mobile) number, an email address, a billing address or a special ID number.
2. The purchase information are the data linked to the expected service, as the SP name, purchase details, purchase currency, purchase date and time.
3. The banking information include the issuer bank name, the Personal Account Number (PAN), the card expiry date and the cryptogram CVX2.

Additional information on the client's browser can also be captured at each transaction (typically to determine the ability to support authentication in 3D-secure) as the IP address, the browser language and time zone, browser screen information or also geolocalization data (particularly in the case of a mobile device).

Four actors are present in electronic payments (Fig. 1): The client wants to purchase an online service with a payment card, through the website of a service provider SP. These two actors have each one payment provider: the issuer and the acquirer bank. In most of e-payment architectures, a fifth actor is involved, the trusted party as a third-party cashier or the Directory used in 3D-Secure. The role of this fifth actor is consequently, various and strongly depends of the architecture.

Independently to the transaction, the issuer bank knows identity information of the client (maybe not all this information) and their related banking information. During the transaction, the merchant knows all purchase information, but does not necessary knows the identity of the client who realize this transaction (and particularly his/her banking information). More generally, it is suitable that in the case of an architecture with a fifth actor, this actor does not acquire more information than necessary (and ideally no personal information, as in a honest-but-curious model).

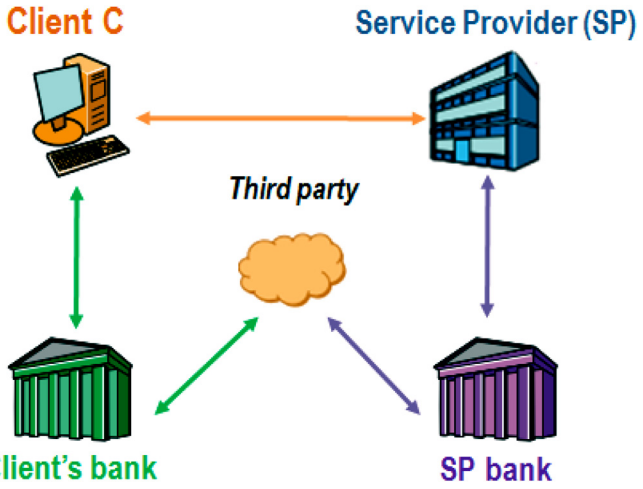

Fig. 1. Actors involved in e-commerce architectures.

A list of security and privacy requirements, including risks raised in the literature [19,22], is established. It also includes a necessary requirement on deployability of the architecture (for example describing if the system is realistic or user-friendly). These requirements have been determined after a security and privacy audits on authentication protocols on common e-payment architectures, as those described in the next section:

- S_1: The **confidentiality of transactions** requires that each exchanged data must be encrypted against external entities.
- S_2: The **integrity of transmitted information** ensures that the content of messages have not been altered.
- S_3: The **SP authentication** by the client or by a trusted party ensures the identity of the SP.
- S_4: The **banks authentication** by a trusted party ensures the identity of acquirer and the issuer bank.
- S_5: The **client's authentication** by a trusted party ensures the identity of the client. Depending on the situation, the trusted party can ideally be the issuer bank or another trusted party *where the client is registered*.
- P_1: The **confidentiality of client's identity towards the SP** ensures that a client can access to a service without disclosing his/her identity to the SP (it is waived if the customer wants a home delivery service).
- P_2: The **confidentiality of client's identity towards the acquirer bank** ensures that the SP can deliver a service to the client without disclosing his/her identity to the acquirer bank.
- P_3: The **confidentiality of purchase information** ensures that only authorized persons have access to order information. This requirement includes that the client's purchase is unknown to the issuer bank.
- P_4: The **confidentiality of banking information** ensures that only authorized persons have access to banking data. This requirement includes the fact that the SP does not know the client's banking information.
- P_5: The **confidentiality of acquirer bank** includes the fact that the client does not know the acquirer bank.
- U_1: The **deployability** ensures the credibility of use of the proposed e-commerce architectures, particularly for fraud detection aspect that should decrease the deployability of privacy compliant architectures.