Dmytro KATSIDYM[1], Svitlana CHAPLINSKA[2]

Opiekun naukowy: Yuriy LAKH[3]

ZAPEWNIENIE BEZPIECZEŃSTWA INFORMACYJNEGO W BANKOWYM SYSTEMIE PŁATNOŚCI ELEKTRONICZNYCH

Streszczenie: W referacie rozważono główne zadania i wymagania dotyczące bezpieczeństwa informacji bankowej w elektronicznym systemie płatności. Zaprezentowano implementację bezpiecznego protokołu 3-D w elektronicznym systemie płatności. Stosowanie niniejszego protokołu zostało przeprowadzone nie tylko po stronie klienta, ale oraz i po stronie serwera.

Słowa kluczowe: elektroniczny system płatności, bezpieczna transakcja elektroniczna, bezpieczny protokół 3-D, smart karta, kod PIN, uwierzytelnianie danych

INFORMATION SECURITY ASSURANCE OF BANKING ELECTRONIC PAYMENT SYSTEM

Summary: The main tasks and requirements for the bank information security in the electronic payment system (EPS) have been considered. The 3-D Secure Protocol implementation in the EPS has been presented. The application of this Protocol has been carried out not only on the client's side, but also on the server's one.

Keywords: electronic payment system (EPS), secure electronic transaction (SET), 3-D secure protocol, smart card, PIN-code, data authentication

1. Introduction

The chosen research theme was caused by the rapid development of technologies and opportunities offered by them. Performing electronic payments is one of such opportunities. Consequently, there is a need to ensure the reliability and security of these transactions. The banking strategy for information security has certain differences from similar strategies of other organizations and companies due to public

[1] Lviv Polytechnic National University, Faculty of Computer Technologies, Automation and Metrology, Information Security department: dimafriend2008@gmail.com
[2] Lviv Polytechnic National University, Faculty of Computer Technologies, Automation and Metrology, Information Technologies Security department: ch.svieta@gmail.com
[3] Lviv Polytechnic National University, Faculty of Computer Technologies, Automation and Metrology, Information Security department: yurii.v.lakh@lpnu.ua

activity of banks, because for the convenience of clients access to funds on the accounts should be very easy as well as due to the specific nature of the threats.

The purpose of the work is analysis of the conditions of electronic payments, classification and characteristics of payment including Internet systems, implementation of an additional protection level in the electronic payment system of the banking institution.

The research object is the structure of information security setting in the electronic payments system, providing additional factor for electronic transactions authentication.

The subject of study is using of 3-D Secure XML protocol as a second authentication factor, consideration of the initial version 3-D Secure 2.0 as well as the necessary conditions, methods and means for its implementation.

2. Key tasks and requirements for the protection of banking information in the System of Electronic Payment (SEP) in Ukraine

During internet-bank payments a new form of payment instruments is used as an electronic payment document. Such a document has a predetermined form and appropriate means of protection provided by the National Bank of Ukraine (NBU) for each SEP participant. In addition, each bank-member of the SEP may have its own system of internet-bank settlements.

The SEP security system is designed to take into account the following requirements:

- The system of protection covers all stages of development, implementation and operation of the software and hardware in a SEP complex;
- The security system includes organizational, technical, hardware and software protection;
- The system has clearly distributed responsibility for the various stages of processing and execution of payments.

The following main SEP protection tasks are provided in the system:

- Protection against unauthorized decryption of messages, the appearance of false messages;
- Automatic logging of the use of the banking network to localize the malfactors from the technology work in the SEP;
- Protection against technical failure of hardware and software tools, the emergence of interference in communication channels.

The SEP security system is multi-staged. It does not include means of information encryption at its different levels, but also contains a range of technological and accounting controls for the transaction of payments in SEP. Technological and accounting control is provided by programs at all levels, which enables the banking staff and customers monitoring the order of payments both during the day and after its completing.

Protection of banking information in the SEP includes a set of actions related to the encryption of information circulating in the payment system. All the files in the SEP are subject to encryption: initial and reverse payment files, receipt files, report files, limit files, correspondent-account status files, and regulatory and reference information files.

3. Static-Data-Authentication, Dynamic-Data-Authentication and combined approach

The Europay, MasterCard, Visa (EMV) transaction contains four basic steps. The first one is to read the needed data from the terminal card for processing. To perform this, the terminal requires for a chip card with the required data. The next step is to verify the card authenticity. For that there are three approaches called Card authentication Methods (CAM): "Static-Data-Authentication" (SDA), "Dynamic-Data-Authentication" (DDA) and "Combined-DDA-with-Application-Cryptogram" (CDA). The third step is to check the card holder by agreement between the card and terminal to select the possible verification method of the card holder. Therefore, a data item for storing the selected verification method is called a CVM (cardholder verifying method). Usually possible approaches for card holder authenticating is entering a PIN, cardholder's signature or nothing at all. The last step is authorization for the transaction. For this purpose the terminal will confirm that the cardholder has sufficient balance for the current transaction.

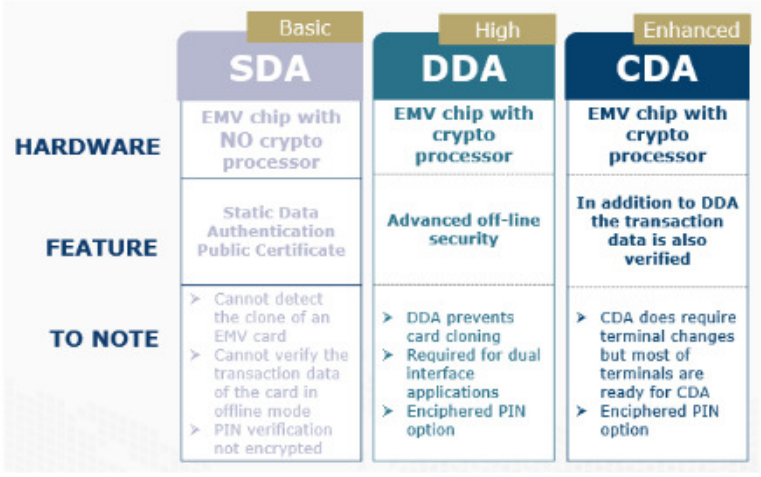

Figure 1. Methods of Card Identification: Static-Data-Authentication (SDA), Dynamic-Data-Authentication (DDA), Combined-DDA-with-Application-Cryptogram(CDA)

4. Card not present transaction (CNP)

CNP involves the performing transactions without presenting the card to the seller and is usually carried out via the Internet or telephone. Because of the absence of physical POS terminals in this type of transaction there is no standard card holder authentication process and this is the main issue that concerns security transactions with CNP.

Despite all the security problems in transactions CNP, fraud CNP is only "one" of the several types of fraud. Other cheatings are classified as "first-party fraud",

"falsifications fraud", "fraud with stolen maps", "fraud by mail and non-receipt" and "theft".

The CNP is divided into two main approaches: the first approach is the protocols based on EMV to ensure that the client at the time of the transaction must have its own card. Authentication of this type of protocols is the so-called two-factor authentication i.e. smart card and password such as Secure Electronic Transaction SET/EMV and EMV/CAP (Chip Authentication Program). In the second approach, the client does not have to have a card during a transaction, for example 3D Secure (usually called 3D Secure and is initially called as a "verified visa" or "MasterCard-Secure-Code").

3-D Secure is an XML protocol used as an additional layer of security for online credit and debit cards, two-factor user authentication but does not guarantee the security of funds on the card. The technology was developed for the Visa payment system in order to improve the security of Internet payments within the framework of the Verified by Visa Service (VbV). Services based on this Protocol have also been accepted by MasterCard payment systems called Mastercard Secure Code (MCC). American Express added 3-D Secure November 8, 2010 as the American Express Safe Key in some markets and continues to implement it in some other additional markets.

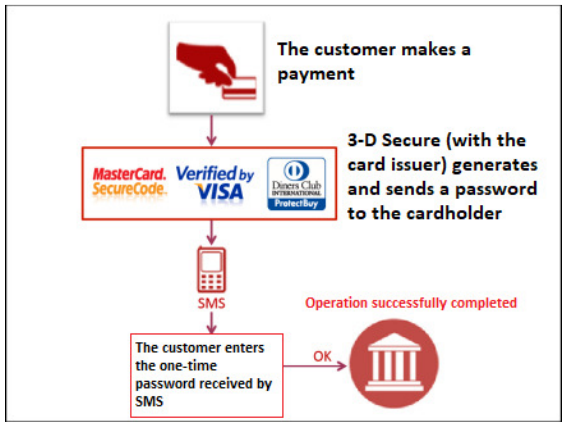

Figure 2. Payment process with 3-D Secure

5. 3-D Secure components

Figure 3 illustrates interactions in the ecosystem EMV 3-D Secure.

3-D Secure includes two authentication streams:
- Frictionless Flow,
- Challenge Flow.

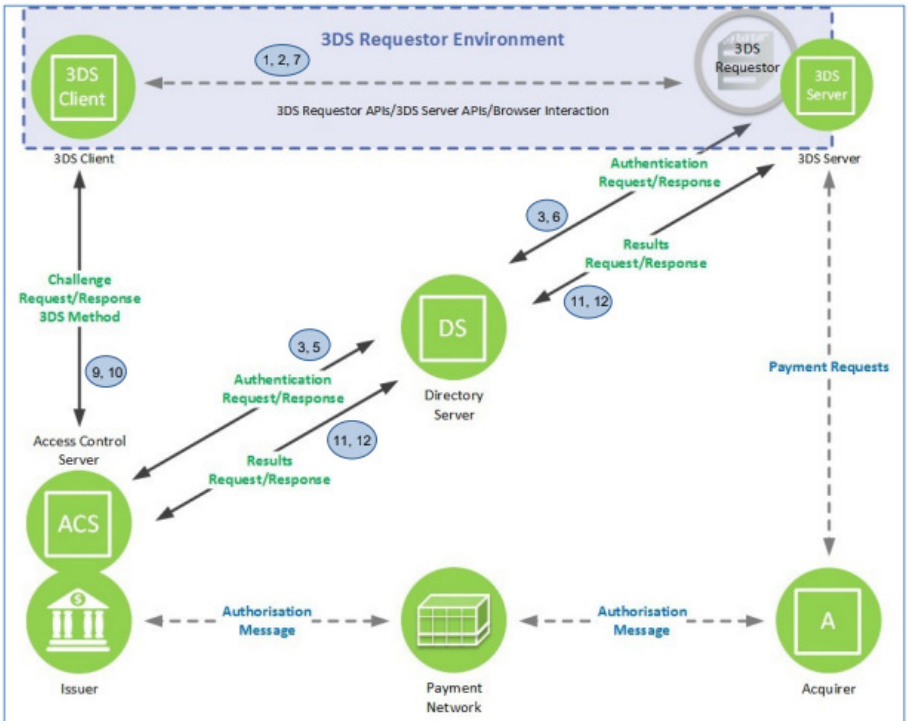

Figure 3. Interactions between EMV 3-D Secure components

6. Client-side implementation

3-D Secure implementation on the client side consists of three main parts:

- creating a Client token,
- create a validation page to collect client's payment information,
- credit card and amount verification using Verify Card Method.

7. Server-side implementation

To create a 3D Secure transaction, one must create a server-side sale using the payment method that was received from the customer during the credit card verification:

```
result = gateway.transaction.sale(
  :amount => "50.00",
  :payment_method_nonce => nonce_from_the_client,
  :options => {
    :submit_for_settlement => true
  }
)
```

The Nonces payment method will include 3D Secure information such as liability_shifted and liability_shift_possible. This is used to validate server risks before generating a transaction.

```
payment_method_nonce                                    =
gateway.payment_method_nonce.find("nonce_string")
info = payment_method_nonce.three_d_secure_info
if info == None:
    return # This means that the nonce was not 3D Secured
info.liability_shifted
info.liability_shift_possible
info.enrolled
info.status
```

The operations also demonstrate 3D Secure information. This could be used to report details of a 3D protected transaction after creating it.

```
transaction                                             =
gateway.transaction.find("the_transaction_token")
info = transaction.three_d_secure_info
if info == None:
    return # This means that the nonce was not 3D Secured
info.liability_shifted
info.liability_shift_possible
info.enrolled
info.status
```

3D Secure 2.0 (3D 2.0) is the next iteration of the 3D authentication protocol. It satisfies the requirements of Strong Customer Authentication (SCA), which come into force in 2019 for European traders carrying out transactions with European customers.

Firstly, the protocol allows to transmit more data elements to issuing banks, which allows them to implement a more effective risk assessment for this authentication. As a consequence, issuing banks will be able to allow more authentications to continue without appealing to the card holder.

Secondly, the authentication itself is designed to be more efficient and secure, especially for mobile devices, leading to fewer authentication-related issues and less waiting time while checking processing.

To reduce the requirement of issuing banks to invoke cardholders to authenticate using 3DS 2.0, better to send some new parameters when calling the card verification method (verifyCard ()):

bin: Numeric identification number of the bank (BIN) associated with the nonce. The tokens received in the object of detail are obtained from the payload;

extraInformation: Additional elements of customer data transferred to the issuing bank. For best results, you should provide as many of these elements as possible. This may require updating the user interface to collect additional information;

onLookupComplete: Need a callback that will be called before the call flow. Accepts two parameters:

- data: THE 3DS Data Retrieval Response object,
- Next: callback function that is performed after 3DS data is used.

```
threeDSecure.verifyCard({
  amount: '100.00',
  nonce:      NONCE_FROM_INTEGRATION,      //      Example:
hostedFieldsTokenizationPayload.nonce
  bin:        BIN_FROM_INTEGRATION,        //        Example:
hostedFieldsTokenizationPayload.details.bin
  additionalInformation: {
    billingGivenName: 'Dima',
    billingSurname: 'Katsidym',
    billingPhoneNumber: '0805607080',
    billingAddress: {
      streetAddress: 'Lukasha M.',
      extendedAddress: '#4', // When available
      locality: 'Lviv',
      region: 'Lviv',
      postalCode: '79007',
      countryCodeAlpha2: 'UA'
    },
    email: 'supermail@protonmail.com'
  },
  /**
  * @function onLookupComplete
  * Newly required in `verifyCard` options object, will be
called after receiving ThreeDSecure
  * response, before completing the flow.
  * @param {object} data - ThreeDSecure data to consume before
continuing
  * @param {string} data.paymentMethod.nonce - payment nonce
  * @param {object} data.threeDSecureInfo
  * @param {boolean} data.threeDSecureInfo.liabilityShifted
  *                      @param                      {boolean}
data.threeDSecureInfo.liabilityShiftPossible
  * @param {function} next - callback to continue flow
  * */
  onLookupComplete: function (data, next) {
    // use `data` here, then call `next()`
    next();
  }
}, function (err, response) {
  // Handle response
});
```

8. Conclusions

It is established that implementation of Protocol 3-D Secure complements another additional level of protection due to the need for confirmation of electronic payment. This allows protecting against fraud of users of the chain: customer-bank-seller.

As far as an authorization factor via SMS message is not reliable and could be easily tapped information, so the authors recommend confirming the transaction through a secure channel connection with the bank telephone application.

Acknowledgement

The research had been performed in the framework of International Project of CRDF Global "IT Audit Cybersecurity", supported by the U.S. Department of State, the Bureau of European and Eurasian Affairs.

Grant Agreement: S-LMAQM-18-GR-2301

.

REFERENCES

1. HANKERSON D.R., MENEZES A.J., VANSTONE S.A. Guide to elliptic curve cryptography. Springer Science & Business Media, 2004. Web-page: *https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.394.3037&rep=rep1&type=pdf*
2. SOLAT S. Security of Electronic Payment Systems: A Comprehensive Survey (January 2017). Web-page: *https://arxiv.org/abs/1701.04556*
3. EMV Co. EMV Book 2 – Security and Key Management – Version 4.1z ECC – With support for Elliptic Curve Cryptography (May 2007).
4. Strengthening Card Authentication: a migration to DDA. An SPA White Paper (July 2015). Web-page: *https://www.smartpaymentassociation.com/images/news/15-07-06-SPA-DDA-Authentication-Final.pdf*
5. 3-D Secure - SDK Specification (October 2019). Web-page: *https://www.emvco.com/emv-technologies/3d-secure/*