INFORMATION SYSTEMS IN MANAGEMENT

Information Systems in Management (2013) Vol. 2 (2) 136−145

PROPOSAL OF A NEW METHOD FOR E-BANKING AUTHENTICATION BASED ON FINGERPRINT READER

ARTUR HŁOBAŻ, KUBA OWSIŃSKI

Department of Physics and Applied Informatics, University of Lodz

The paper presents a novel method/mechanism for electronic banking transactions authentication based on biometrics, using fingerprint reader. The method allows to identify the client not only by something that he has or knows, but who he is. Therefore, the proposed solution enhances security of transactions authentication by an additional factor of client identification - this kind of solution hasn't been currently used by banks in Poland so far. The article also presents that the application of an additional level of security is not associated with an increase of costs for banks but allows them to reduce them, especially for long-term relationships with customers.

Keywords: Electronic banking, Authorization codes, Authorization, Biometric data, Fingerprint scanner

1. Introduction

Banking, like many aspects of our lives, moved to the Internet. Clients are increasingly willing to use this method of payment and control of their finances because of the convenience and time savings [1]. However, with the popularity of the Internet and electronic banking has increased the number of attacks and extortions by online criminals [6,7,8,9]. Hacking attacks on bank servers are just one of the methods. Statistics show that much more effective attacks are directly in the client. It mostly often happens through e.g. substituting a fake login webpage of the bank and extortion of authorization data. Banks increase security by encrypting connections, masking passwords or detection of failed logins. However, the most effective

to approve operations with a high degree of risk are authorization codes, such as transfers to external clients or changing personal information of the client in the bank system [2].

The purpose of this article is to present a new method of banking operations authentication in the telecommunications banking services area. Due to the diverse needs of retail and corporate customers in the article will be taken into account only the services offered to individual customers.

2. Device selection

For the tests, the Transcend JetFlash 220 4GB device was selected, which already includes software to read the fingerprint pattern and validate it. Manufacturer software protects access to the disk using 256 bit key (AES) [5]. During the first start up of the device the client is asked to scan a fingerprint and after that while every next starting the device will ask for moving the finger through the scanner and will verify fingerprint. Only after positive comparison, the client will have access to the device on which the generating codes application is stored [3, 4].

The authentication system consists of a client application running on the client machine, which is activated from the JetFlash 220 device, and application on the server running on the bank side. Client application does not perform data validation but verify only their format and their length. After that the data are sent to the server and client receives back the answer.

3. Client application

The task of the client application is only to obtain relevant data from the client and send them to the server (Fig. 1). The data, which will be sent, are:

ID – unique device serial number. This number will be read each time from the device's memory. It is essential to the production stage, that this number has to been stored in device memory with no possibility of modifications. It will be read from the device and assigned to a particular user at the time of delivering the device.

CIS – the same number as the ID number in electronic banking. The customer will have to enter it every time because there will not be write access to the device after the production process. Entering CIS number will also provide additional protection.

PIN – access code which provides additional protection. PIN will be determined by phone call at the time of authentication method activation and will not be stored in memory.

CLIENT IP – IP address of the computer from which the request was send.

DATA OF OPERATION – data set by the bank being characteristic for specific transaction. This could be the last four digits of the account numbers of customers, which are presently used by banks.

Data is encrypted and sent to the server and the client program waits for a response.

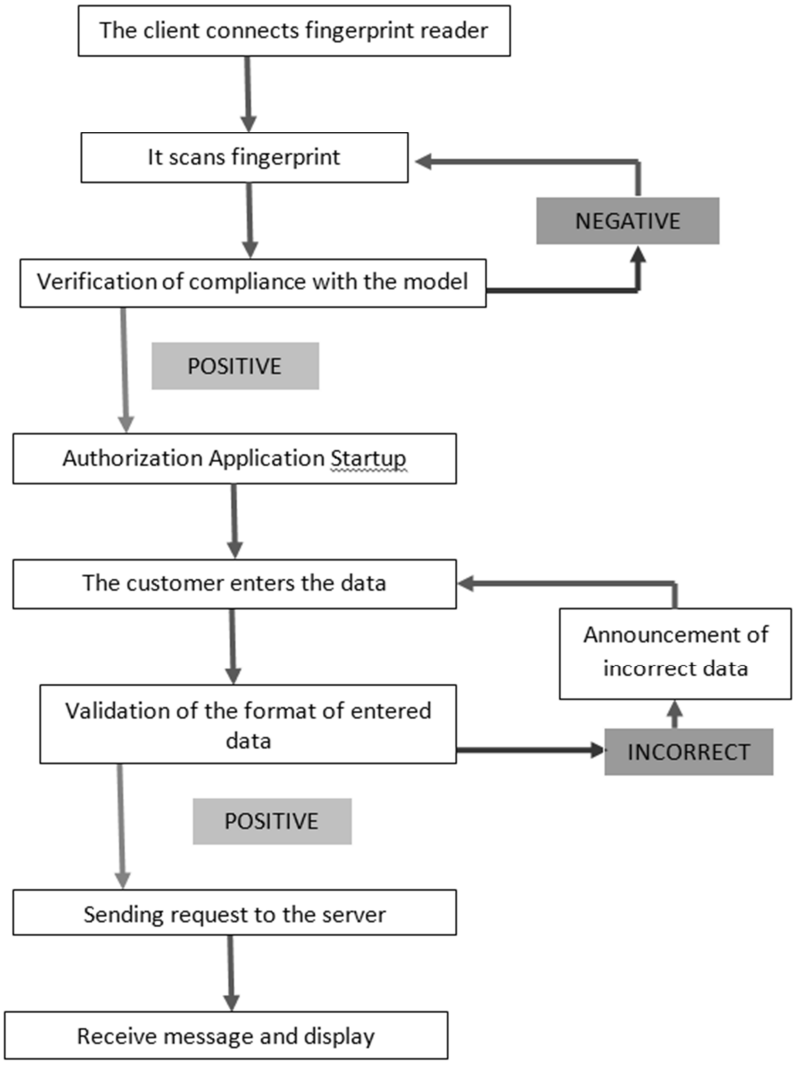

Figure 1. Diagram of the client application - a single code generation

This method is useful for the approval of transactions on the website because the customer who is going to make the transaction in such a way, must have access to a computer with Internet. In addition, it is possible to generate not just one code, but also a list of codes.

4. Server application

The server waits for a response, ensuring uninterrupted operation and support for multiple clients simultaneously. The application receiving a client request first check whether the customer actually performs an operation that requires authentication. The purpose of this is to protect the server from the load due to the generation of unnecessary codes. Next is being verified whether the customer has activated the biometric tool and the CIS or the ID of the device is not blocked. A further step is to verify that the client uses its own device and introduces the correct PIN. The last step is to check the transactions data and generate an authorization code (Fig. 2a and 2b).

The similar schema of action is in the case of receiving a request of code list generation. In addition to data validation is to verify the expiration date and the number of codes that the client wants to receive. This is the stage of generation, which can be freely modified by the bank.

5. Method of device activation

Device delivery to the customer can be done by sending it from the bank's head office directly to a particular client or to individual bank branch where the client can get it in person. The second method is preferred for two reasons. Firstly is cost, because of the small dimensions of the device it will be cheaper for bank to deliver package containing several devices to a single address (bank branch) than the delivery of each device to a separate addresses of clients. Secondly there is the need to wait by the client for the delivery while the bank's branches can create supplies and give the device, for example, in the moment of opening an account by the client.

Regardless of how the equipment will be given to the client, it should be preassigned to him. The proposed method is coding ID of device in the bar code. The bank clerk before issuing or delivery the device, scan the bar code and into this way assigns it to the client. The label with the bar code should be peeled off before giving the device to the client for safety reasons.

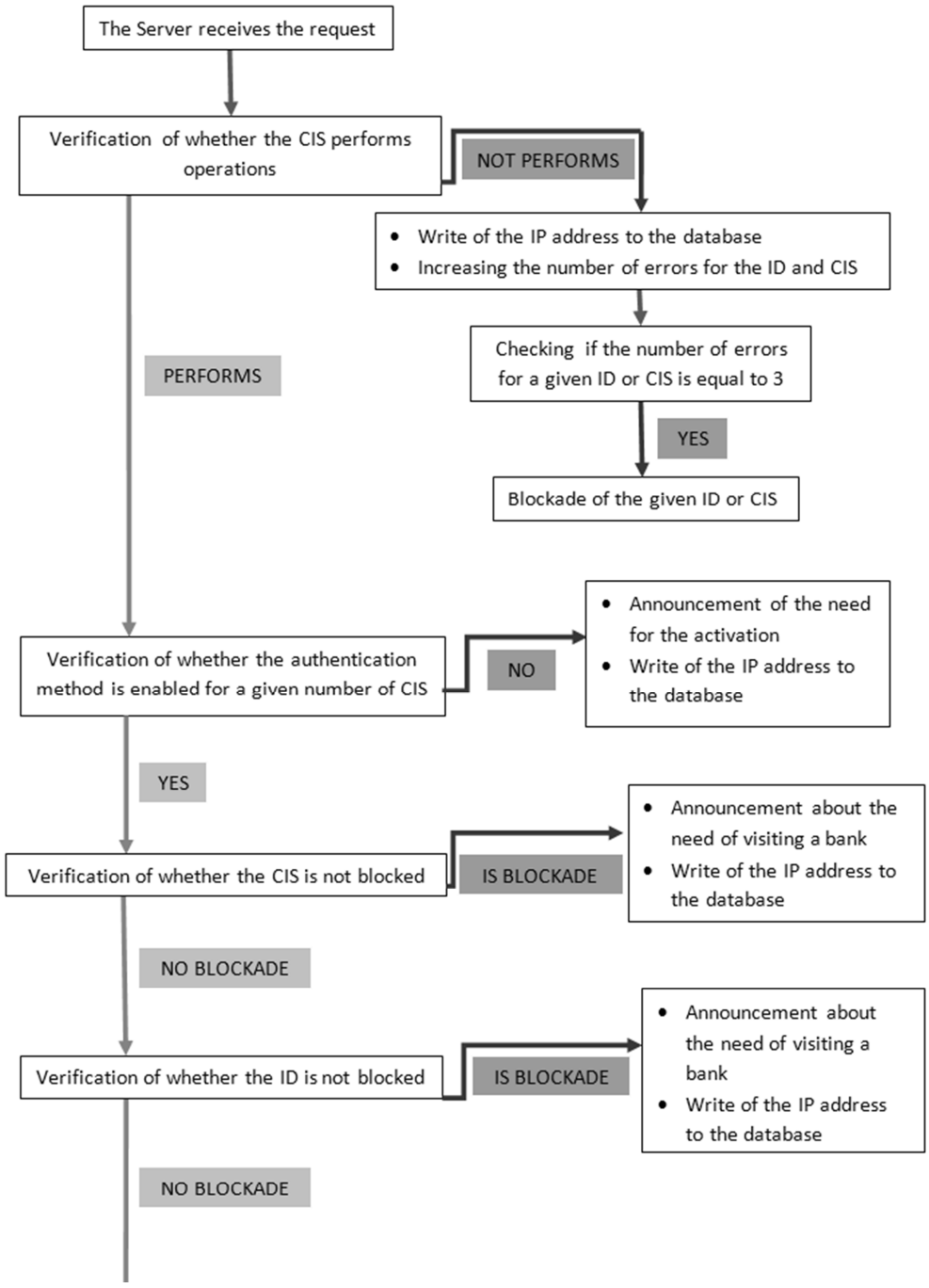

Figure 2a. Diagram of the server application if it receives a request for code generation

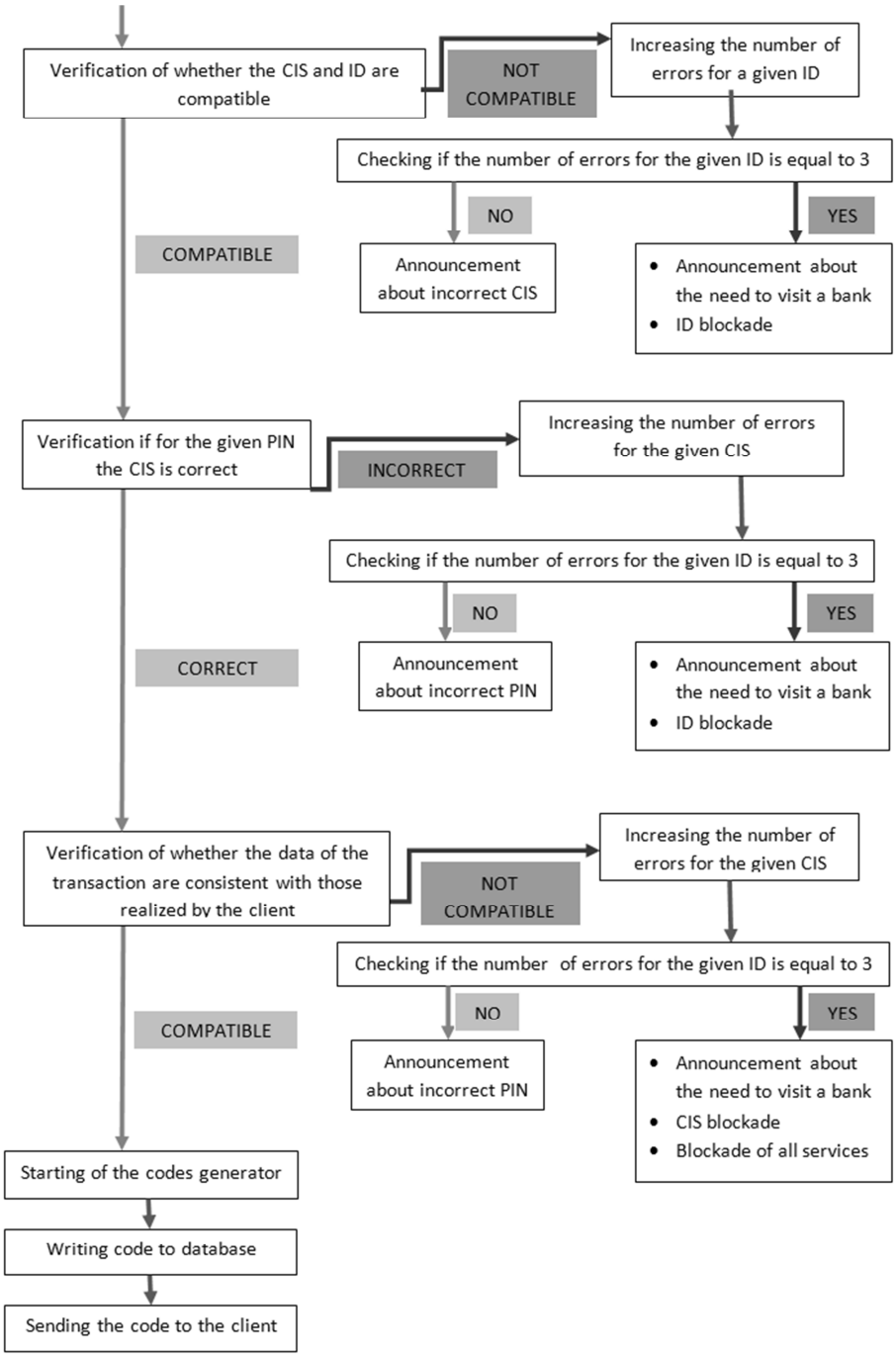

Figure 2b. Diagram of the server application if it receives a request for code generation

On the telephone number, specified by the customer in the bank facility, contact call center employee who verifies the client (for example, by logging in to the telephone service) and sets with him the PIN to a biometric tool. The client enters the PIN on the phone, which is stored in a database. This method of PIN generation is nowadays being used by banks to determine PIN to hardware token, credit card or telephone services.

During the first start of the device client folds the fingerprint pattern, runs the application and generates the first code, which enters on the bank website in the section of the authentication settings. If the generated code is correct, biometric device is activated and becomes the only way to authorize the operation of the client.

6. Comparative evaluation of the security

Nowadays offered methods have different levels of security. They can be based on what the customer has (e.g. the card with one-time codes, cell phone with number on which SMS with code comes) or/and knows (e.g. PIN code). The third level of security is based on a hidden data. In the case of a hardware token client must have a device, knows PIN and the generation of the code is done on the client and server side on the base of serial number stored on both sides, however not known for the user - it minimizes the risk of extorting this data from the client [2].

The proposed solution introduces a fourth level of security, which until now has not been used to authenticate banking transactions. In summary, the security of authorization code generation is based on four characteristics:

1. something that the client has - biometric device,
2. something that the client knows – PIN,
3. something that is assigned - the unique ID of the device which is unknown for the client,
4. something that confirms the identity of the client – fingerprints.

Clearly it can be concluded that the proposed method offers the highest levels of security and the information on which the authorization codes are generated.

7. Comparison of the costs of methods

Because it is not possible to estimate the cost of a single code generation for every method, the best indicator of the cost will be incurred in generating a number of codes in a given period of time. The following simple analysis of the expenses of each authorization method for one user will be made in the period of one (Fig. 3), twelve (Fig. 4) and thirty six (Fig. 5) months. A generalized value of 20

operations per month was assumed for each of them. It is not excessive, especially since more and more banks will require an authorization code not only to approve financial transactions, but also for the login to the website, for example to see the account balance.

On the basis of analysis of the charges in selected Polish banks [10,11,12,13,14] assumed average prices for the most popular authorization methods nowadays:

- **Card of codes** - issue the card of codes for 50 operations is an expense of 5 zł [12].
- **SMS codes** – it was assumed that the cost of one SMS is 0.20 zł (0.20 zł x 20 operations = 4 zł) [11, 13].
- **Hardware token** - generates a fee for the issuance of 48zł and 1zł for monthly usage [15].
- **Biometric token** - the purchase price of a single device of Transcend JetFlash 220 4GB for retail client is 51,30 zł (www.saturion.pl; January 2013). It is important, that the costs can be further reduced by a significant reduction in memory capacity and mass production. It was assumed that the customer will not be charged monthly fees by the bank for the use of biometric token.

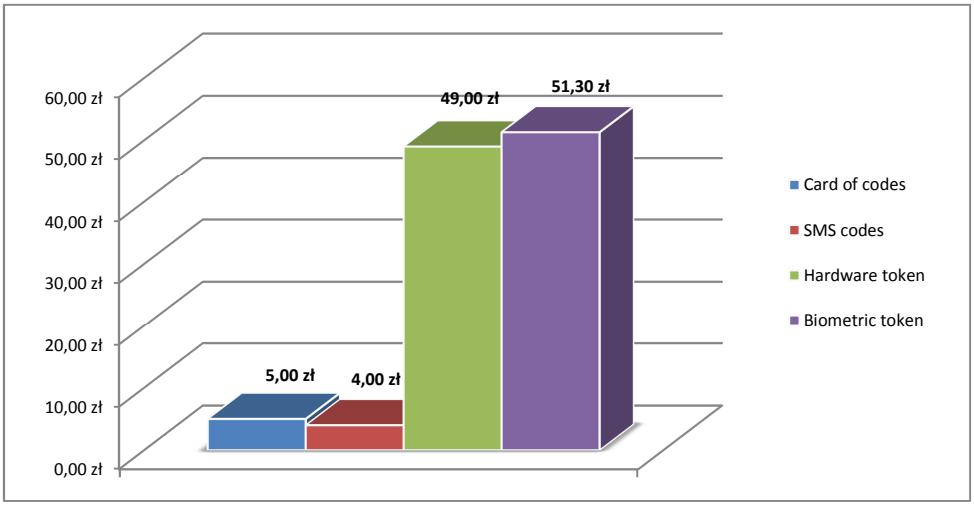

Figure 3. Costs of 1 month using of chosen authorization methods for one customer

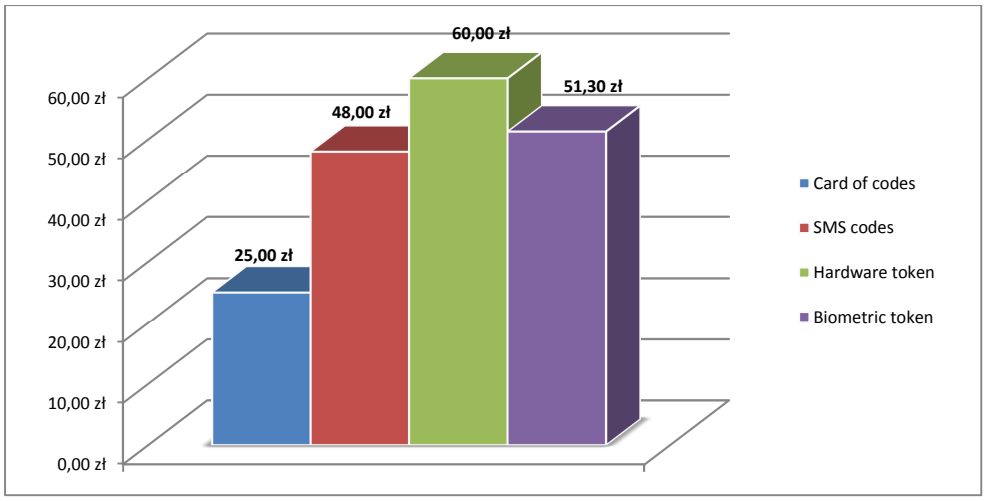

Figure 4. Costs of 12 monthly using of chosen authorization methods for one customer

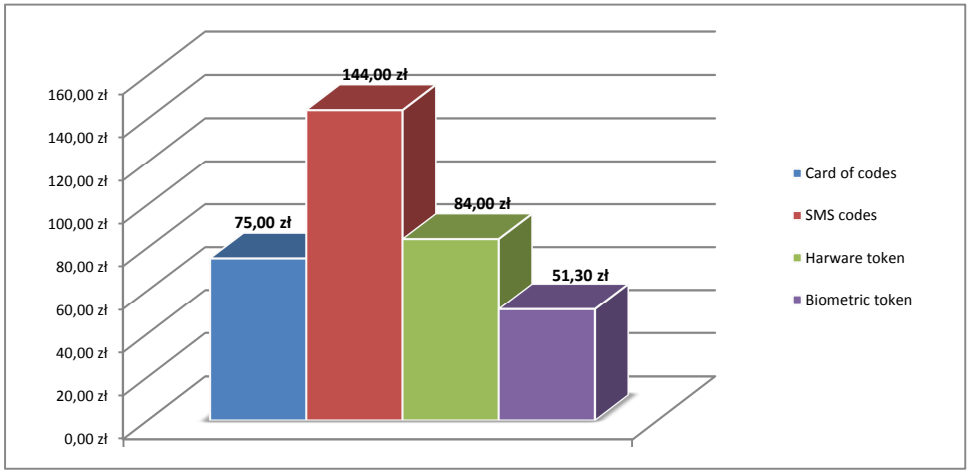

Figure 5. Costs of 36 monthly using of chosen authorization methods for one client

8. Conclusions

This paper proposes a new method for banking authentication that uses a fingerprint reader. It is important that the new solution provides a higher level of security and convenience of service, while reducing costs in the long term use. The implementation of biometric token by any of the banks will add not only additional authentication method to choose from, but the solution cheaper, safer and higher level of prestige and functionality.

REFERENCES

[1] Matuszyk A., Matuszyk P. (2008) *Instrumenty bankowości elektronicznej*, CeDeWu Centrum Doradztwa i Wydawnictw.

[2] Anderson R. (2006) *Inżynieria Zabezpieczeń*, Wydawnictwa Naukowo – Techniczne.

[3] Bolle Ruud M., Connel Jonathan H., Pankanti Sarath, Ratha Nalini K., Senior Andrew W. (2010) *Biometria*, Wydawnictwa Naukowo – Techniczne.

[4] Ślot K. (2008) *Wybrane Zagadnienia Biometrii*, Wydawnictwa Komunikacji i Łączności WKŁ.

[5] Menezes A., Oorschot P., Vanstone S. (2005) *Kryptografia Stosowana*, Wydawnictwa Naukowo – Techniczne.

[6] Portal Niebezpiecznik.pl (stan na dzień 01.06.2012r.) *Phishing na klientów ING*, *http://niebezpiecznik.pl/post/uwaga-na-phishing-na-klientow-ing/*

[7] Portal Niebezpiecznik.pl (stan na dzień 01.06.2012r.) *Phishing na klientów BZ WBK*, *http://niebezpiecznik.pl/post/phishing-skierowany-w-klientow-bz-wbk/*

[8] Portal Niebezpiecznik.pl (stan na dzień 01.06.2012r.) *Atak „Zeusa" na klientów bankowości internetowej, http://niebezpiecznik.pl/post/zeus-straszy-polskie-banki/*

[9] Portal Niebezpiecznik.pl (stan na dzień 01.06.2012r) *Kradzież danych tokenów RSA*, *http://niebezpiecznik.pl/post/wlamanie-na-serwery-rsa-wykradziono-dane-zwiazane-z-securid/*

[10] PKO BP, Tabela Opłat i Prowizji *http://www.pkobp.pl/index.php/id=autom_oppr/subid=auto_249/section=ogol*

[11] PEKAO S.A., Tabela Opłat i Prowizji, *http://www.pekao.com.pl/binsource/f/55/75/bin_P1K073bccb6d03ebb3665575,ATTACHMENT,PL,1,20,0/Nowa_linia_rachunkow_oszczednosciowo-rozliczeniowych.pdf*

[12] MBank, Tabela Opłat i Prowizji, *http://www.mbank.pl/download/taryfy/tpio-21.05.2012.pdf*

[13] Inteligo, Tabela Opłat i Prowizji, *http://inteligo.pl/przydatne-informacje/oplaty-prowizje-i-oprocentowanie/*

[14] ING Bank Śląski, Tabela Opłat i Prowizji, *http://www.ingbank.pl/_fileserver/item/1005012*

[15] PEKAO S.A., Oferowane metody autoryzacji, *http://www.pekao.com.pl/indywidualni/bankowosc_elektroniczna/Bezpieczenstwo/#tab2*

[16] Ostrowski E. (stan na dzień 20.05.2012r.) *Metody i Algorytmy Sztucznej Inteligencji*, *http://sequoia.ict.pwr.wroc.pl/~witold/aiarr/2007_projekty/odciski2/*