Risk in the Internet banking service

Sebastian Bakalarczyk[1]

Abstract

The focus of this paper is on the problem of risk and security in the electronic banking service. A detailed analysis concentrates on the Internet banking service. It shows that security of the Internet banking platform is an inseparable part of the process of risk management in banks. Since banks, just like other organizations, are exposed to different risks they have to be under constant and permanent control. Risk has to be measured, defined and properly managed in order to satisfy the needs of banks and their clients. Risk management process has to be systematically planned in the long term. The paper provides for a review of the literature and historical development of key concepts.

Key words

Risk, Internet, banking, service.

JEL Classification: G21

1. Introduction - general overview

Electronic banking is a service offered by banks and enables its clients to access the account through the computer or other electronic device (for example: Automated Teller Machine or POS) and telecommunications line (for example: phone line). Consequently, electronic banking is a modern form of banking service realization that allows banks' clients to conduct financial service without visiting bank's office anywhere in the world. Fast development of electronic banking service was caused by the introduction of Automated Teller Machines (ATM). First device was installed in New York Chemical Bank. At the beginning, ATMs worked in offline mode and they were not connected with any computer networks. Internet banking is the subject not as extensive as electronic banking as it is just one of the forms of it. Internet banking is the process that allows the client to enter his or her bank account with the use of the www technology and simple web browser. The history of Internet banking starts in 1994 in the United States. La Jolla Bank PSB in California was one of the first that opened its Internet branches. In 1995, Security First Network Bank (SFNB) was opened providing only Internet service.

One of the most important factors in the development of electronic banking was the technological revolution that took place by the end of 20th century. The most meaningful changes were in the fields of information technology (IT) and telecommunications that allowed the Polish banks to offer tools, which let its clients to manage money through the Internet. These tools were introduced as a response to the needs of companies and organizations that were conducting more and more transactions with their contractors. As the number of payments was increasing, it became important to pay as late as possible. Moreover, collection of stock was possible only after payment. This raised a need for implementing a new method of contact with the bank. Companies understood how important it is to take

[1] Sebastian Bakalarczyk, PhD, Lodz University of Technology, Poland, EU, s.bak@p.lodz.pl

advantage of new tools as they allowed cutting costs of work and increasing the effectiveness. Consequently, this led to dynamic development and predominance over the competitors.

2. The Attributes of Safety in Electronic Banking Operations

The safety of electronic banking is strongly connected with the problem of client's distrust when it comes to new technologies since many of new threats appeared together with presence of electronic channels of banking service distribution. According to the research of CBOS in 2008, more than 80% of Poles are convinced that electronic banking service is safe. Electronic banking system can be perceived as safe, when basic attributes of safety reach the level, which is accepted both by the bank and its clients. Among the attributes of safety it is possible to distinguish some basic characters (Wojciechowska – Filipek 2010):

- Confidentiality, which will provide an access to the system only to people who are authorized;
- Integrity, which prevents modifications during the process of data transmission as making the transaction;
- Authenticity, which gives the possibility of the assessment if the person who confirmed the transaction if really the right client;
- Repudiation, which is a lack of possibility of denial of giving or receiving some stated message through electronic channels;
- Availability, which is an uninterrupted access to the system of electronic banking;
- Reliability, which is a right operation of the system.

According to the above attributes of safety, it is possible to apply potential threats of electronic banking to the concept of four types of attacks on IT system: interruption, the threat of the availability; interception, the threat of the confidentiality; modification, the threat of the integrity, and counterfeiting, the threat of the authenticity.

2.1 Cryptography in Electronic Banking Service

In the Internet Banking all connections between the client (client's browser) and the bank (bank's server) are encrypted. Cryptography is a process of transferring the data in masked form so that only the addressee would be able to read the message. Moreover, the recipient has to be sure that the message was not modifies by anyone.

The message that has to be sent is called public message or open and the process of hiding is called coding. As a result of coding a cryptogram is created and it is possible to read it only by means of decoding. Cryptographic algorithm, also called code, is a mathematical function used for coding and decoding. In order to code a public message it is necessary to use an encryption algorithm. Consequently, to decode the message, decryption algorithm must be used. If a security applied in the algorithm is based on protecting the content, it can be assumed that a limited algorithm is created. Currently, limited algorithms are no longer used as they provided insufficient protection.

Modern algorithms offer the security ensured by the application of the key. It is possible to distinguish two groups of algorithms, where keys are applied: symmetric algorithms and algorithms with public keys. In symmetric algorithms, encryption key is determined based on decryption key and the other way round. It often occurs that both keys are the same.

These algorithms are, also, called algorithms with confidential key or algorithms with single key. In this case it is required to adjust a key between sender and recipient before the transmission of the message. Keeping the key in secret is a guarantee for safe data transmission. A completely different group are algorithms with public keys, which are called this way as encryption key can and even has to be revealed in order to allow other people coding the message, which reading is only possible by using decryption key. Consequently, only the owner of decryption key (the recipient) is able to read the message, of course if he or she did not reveal the key.

Cryptosystem is every system, where encryption transformation assigns each unit of the public content the unit of encrypted message. Moreover, decryption transformation performs the public key from encrypted message. This kind of system is characterized by: encryption transformations and decryption are efficient for all keys, and security of the system depends on the confidentiality of the key, not on the confidentiality of the key (Jaźwiński, Ważyńska-Fiok 1993).

Cryptosystems are characterized by different levels of security. In theory, each algorithm can be broken, however, in practice, it is not always possible. There are a few basic types of algorithms and cryptography methods.

2.1.1 Data Encryption Standard Algorithm and its Modifications

Data Encryption Standard (DES) code is a symmetric algorithm, where in order to code and decode only one key is required. The algorithm operates in series; it codes binary numbers 64 bit with the use of 56 bit key. Coding operation is the operation of submission of a modulo of two fragments with public text with the fragment of the key. This operation is conducted on 48 bit data blocks. Data block is divided into two equal parts (32 bit each) in order to obtain 48 bit form. After that, the block is under the influence of expansion permutation. In every of sixteen steps, the process of coding applies to a half of the data word, left and right side are coded one after another. 48 bit key is created based on transfers and permutations, which are narrowed by creating 48 bit under key based on the 56 bit. For each iteration of coding the original key is created based on the periodical transfer of basic key bits. After the operation of sixteen coding operations the function of encryption is continued in so-called s-boxes allowing to transfer the text of 48 bit by 32 bit. The operation of encryption is finished by the inversion of the introductory permutation applied on the data block before the beginning of the encryption operation. Decryption operation is conducted based on the previous steps but in the other way round. The key to each next operation is prepared based on the partially prepared key for previous operation. Consequently, when the user wants to obtain the key of the second iteration, it is necessary to, firstly, create the key of the first iteration etc. For each operation of encryption, a separate, private key is created. While preparing the key it is necessary to apply two operations: transposition (permutation) and periodical transfers. The preparation of data is conducted with the use of permutation operations and data division into two equally parts. On each of sixteen iteration of encryption, symmetrical sum is applied. Final operations bring the 64 bit form to the data (Stallings 1997).

2.1.2 International Data Encryption Algorithm

International Data Encryption Algorithm (IDEA) operates on 64 bit blocks using 128 bit key. Based on this key, 52 sub key are generated, each has 16 bit. The generation is conducted as follows, firstly, the key is divided into eight 16 bit parts. They create first eight keys. Secondly, 128 bit key is periodically transferred by 25 bit in left (25 the eldest keys enter again to the right side) and immediately, next eight sub keys are broken. Finally, in 17th round there are only four keys chosen from the side of the eldest bits. Encryption with the use of IDEA is conducted in 8 rounds so this is a complex algorithm, however, this is not the network of Feistel type (symmetric structure used in the construction of block ciphers, DES code is based on it (Bono et al. 2005)). In each round, six keys are used. In each of the rounds, the block is broken into 16 bit quarters, which are connected by three incompatible operations. Each of these operations processes only 16 bit numbers. As a consequence, it is easier to implement IDEA as equipment. Moreover, it works efficiently even on 16 bit processors. At the end, on four blocks, 16 bit each, it is necessary to do the final transformation by means of last four keys and set them as a cryptograph.

2.1.3 RSA Algorithm

RSA is an encryption algorithm, which has two keys: public used for coding of information and private used to reading them. Public key allows to encrypt data but it does not let the user to read the information, consequently, it does not have to be protected. Thanks to this code, companies that allow their clients to conduct Internet payments can protect them from attacks. On the other hand, private key is used for reading the information, which has been coded by means of the first key. In addition, this key is not publicly available. RSA system allows safe data transfer in the environment, where some abuses are possible. The security is based on the difficulty of distribution of high numbers on prime numbers.

There are three stages of RSA algorithm. Firstly, there is a generation of public and confidential key. Public key is transferred to all interested parties and allows data coding. Confidential key allows data decoding, which has been coded by public key. Second step occurs, when the user receives a public key, for example: by means of the Internet, he or she is able to encrypt its data and send them as a code RSA to the recipient, who has a confidential key. Public key does not have to be protected since it does not allow to decode the information, the process of encrypting is not reversible by means of this key. As a consequence, there is no need of securing it and it can be entrusted to anyone who is interested without any risk. And finally, the recipient, after receiving the encrypted information, can read it through the confidential key.

2.1.4 Diffie-Hellman Algorithm

Diffie Hellman algorithm is a method for securely exchanging a shared secret between two parties, in real-time over an entrusted network. Let us assume that two parties have not communicated previously, shared secret information is important for both of them and they are curious to code their communications. In order to make this situation efficient, it is possible to apply several protocols, including Secure Sockets Layer (SSL), Secure Shell (SSH), and Internet Protocol Security (IPSes). The algorithm is based on simple mathematical calculations since it includes the algebra of exponents and modulus arithmetic. The goal of this process is to allow two users to be able to exchange certain information that suppose to be secured by means of symmetric encryption algorithms.

The Diffie-Hellman algorithm is the technology widely used in the Internet, it covers protocols such as: SSL, SSH, IPSec, PKI. In order to code it is necessary to apply Secure Sockets Layer protocol (SSL). The protocol provides safe communication channel between client and server. SSL is the protocol that has a general application and it is a companion for many different protocols (in case of www service this is HTMS protocol). SSL is based on both the use of asymmetric cryptography (in order to crypt and decrypt the key has to be different and it usually is PSA algorithm with the key of 1034 bit) and symmetric (the key is the same, usually RC4 algorithm with 128 bit).

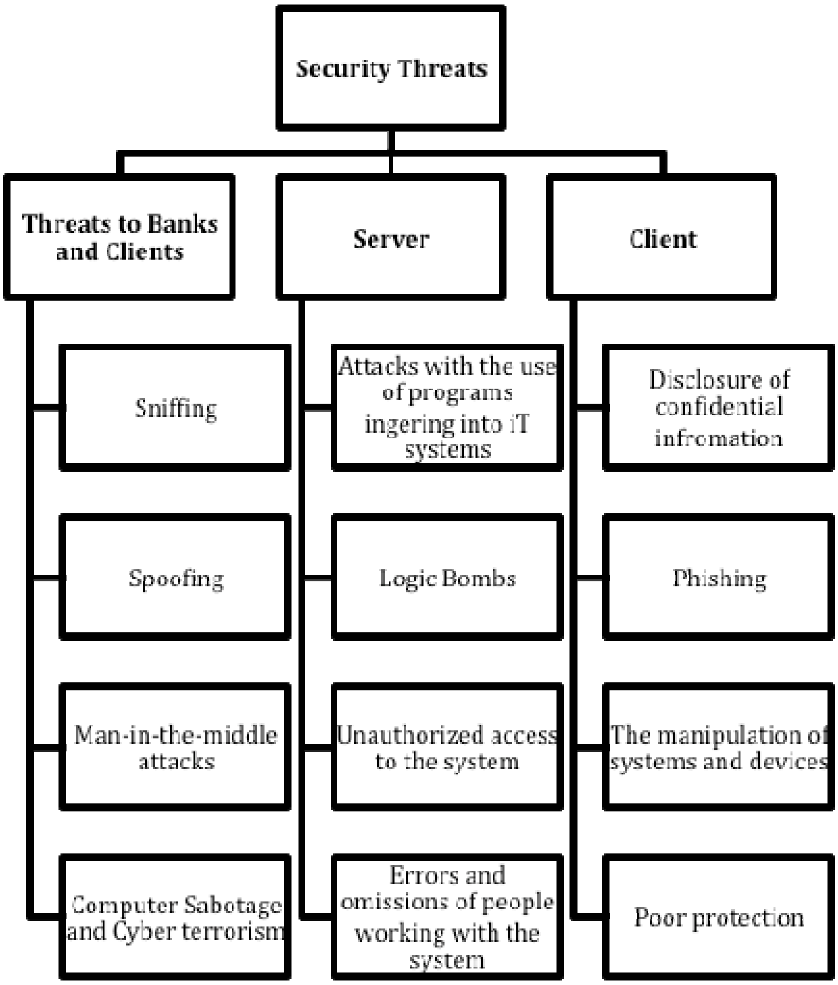
Asymmetric cryptography is only used in order to coordinate the symmetric key applied in further communication. Client’s computer gets the public key from its client and it is used, by this computer, to code the symmetric key and to send it to the server. Further communication takes place with the use of symmetric key and this is connected with the fact that the speed of data coding is extremely high. Symmetric key mediates in this process. Symmetric key is always generated for each separate session, consequently, it is called session key. It seems that

SSL code cannot be broken; however, it has a few weaknesses, which can occur based on the behaviour of the client (Denning 1992).

2.2 Security Threats of Data in Banking Information Technology Systems

Security threats of data in information technology systems are connected with their processing and storage. It is possible to distinguish three basic groups (Bakalarczyk 2012).

Figure 1: Types of Threats in Internet Banking Systems


Security Threats
Threats to Banks and Clients
Server
Client
Sniffing
Spoofing
Man-in-the-middle attacks
Computer Sabotage and Cyber terrorism
Attacks with the use of programs ingering into IT systems
Logic Bombs
Unauthorized access to the system
Errors and omissions of people working with the system
Disclosure of confidential infromation
Phishing
The manipulation of systems and devices
Poor protection

2.2.1 Threats to Bank and Client

Sniffing is the process allowing intercepting and logging traffic passing over a digital network or a part of a network. Usually, to conduct this process it is necessary to apply devices, such as: network analysers, protocol analysers, sniffers, Ethernet sniffers or wireless sniffers. As data streams flow across the network, the device captures each packet and decodes the packet's raw data, showing the values of various fields in the packet, and analyses its content according to the appropriate Request for Comments (RFC) or other specifications (Connolly 2003). All of the analysers have a common characteristics, they are able to switch Network Interface Card to promiscuous, where the device is able to receives are frames from the network, also, those not addresses directly to him. Sniffer can also be run on router or on the computer, which is a part of network communication. In these cases promiscuous is not necessary. Sniffer is usually used by most of the networks' administrators, especially during the diagnosis of problems with reliability of efficiency of links. In can be also applied for the monitoring of the network efficiency of third parties, which is usually against the law. Cryptographic mechanism, described previously, is used by certain communication protocols in order to protect against those attacks.

Sniffer devices ensure the possibility of many different applications, such as: analysis of network problems; detection of network intrusion attempts; detection of network misuse by internal and external users; documenting regulatory compliance through logging all perimeter and endpoint traffic; gaining information for effecting a network intrusion; isolation of exploited systems; and filter suspect content from network traffic, etc.

Spoofing attack is a situation, when a person or program can successfully masquerade as another by falsifying data; consequently, gaining an illegitimate advantage. In order to fully understand the process of spoofing, it is necessary to examine the concept of the communication protocol suite.

The Internet protocols are the world's most popular open-system protocol suite as they can be used to communicate across any set of interconnected networks and are equally well suited for LAN and WAN communications. The most popular communication protocols are: Transmission Control Protocol (TCP) and the Internet Protocol (IP).

Firstly, Internet Protocol (IP) is a network protocol operating at layer 3 (network) of the Open Systems Interconnection Model (way of sub-dividing communications system into smaller parts called layers. Similar communication functions are grouped into logical layers. A layer provides service to its upper layer while receiving service from the layer below. On each layer, an instance provides service to the instances at the layer above and requests service from the layer below). IP is a connectionless model, meaning there is no information regarding transaction state, which is used to route packets on a network. Moreover, there is no method in place to ensure that a packet is properly delivered to the destination.

IP can be thought of as a routing wrapper for layer 4 (transport), which contains the Transmission Control Protocol (TCP). Differently than IP, TCP uses a connection-oriented design. This means that the participants in a TCP session must first build a connection, through the 3-way handshake (SYN-SYN/ACK-ACK) - then update one another on progress, though sequences and acknowledgements. This connection ensures data reliability, since the sender receives positive information from the recipient after each packet exchange.

Both issues lead to the problem of consequences of using IP and TCP. It is not difficult to mask a source address by manipulating an IP header. This technique is used for obvious reasons and is employed in several of the attacks described below. Next consequence, specific to TCP, is sequence number prediction, which can lead to session hijacking or host impersonating. This method builds on IP spoofing, since a false session is built (Gantz et al. 2007).

Internet Protocol spoofing is a problem that still does not found a proper solution as it is inherent to the design of the TCP or IP suite. However, knowledge about the entire process can allow users to prevent from those attacks.

Man-in-the-middle attack (MITM attack) is the attack, when the attacker intrudes into the communication between the endpoints on a network to enter false information and intercept the data transferred between them. MITM attack is also commonly called as: Bucket-brigade attack, fire brigade attack (derived from the fire brigade operation of dousing off the fire by passing buckets from one person to another between the water source and the fire), monkey-in-the-middle attack, session hijacking TCP hijacking or TCP session hijacking (the intruder aims to gain access to a legitimate user's session to tamper it). Originally, the name *Man-in-the-middle* was introduced based on the idea that two baseball players that want to pass a ball to each other while one player between them tries to seize it.

MITM attack often begins with sniffing and eavesdropping on a network stream, and ends with trying to alter, forge or reroute the intercepted information. These attacks are mainly selected by hackers involving public-key cryptosystems. In case of public keys the attacker may make a substitution by changing the intercepted public key by some forged public key. Usually the users of the systems are convinced that they safely communicate with each other. The attacker may apply a program, which is able to appear like a server for the client (Leyden 2003).

MITM attacks are characterized by the fact that the theft aims to enter between two target network endpoints, and proxies all the communication between them. If the process is successful it is very likely that other attacks will take place, such as: sniffing or hijacking already authenticated sessions, injecting packets or commands to the server, and sending the forged responses to the client. Usually, MITM attacks are designed for obtaining very sensitive and important information. These attacks, often, intercept both http or https channels. MITM attacker has to carefully target its victim, as he has to direct the endpoint to the attacker's proxy server not the real server. The goal of these actions is to obtain an access to the victim's messages and modify them. After that the attacker transmits data to the server end. It is also possible that MITM attack would cheat the communicators at the victim or server end in order to obtain some sensitive information, such as: address, passwords or some confidential data. Consequently, the attacker will be able to manipulate transactions.

Man-in-the-browser attacks (MITB) is a form of the attack similar to Man-in-the-middle attack. It is a Trojan horse that inflects a web browser and has an opportunity to interact pages, the content of transactions or add other transactions. The entire process is completely invisible for both parties. The MITB attack can be controlled only by utilising transaction verification.

The attack is based on the idea that the Trojan horse works by utilising facilities provided to enhance Browser capabilities, for example: Extension and User scripts etc. Consequently, the procedure cannot be detected virtually to the scanner of viruses. The analysis of a simple Internet payment transaction indicates that bank's client is always visible through confirmation screens. Consequently, information about the transaction will be entered to the browser. On the other hand, the bank receives a transaction with materially altered instructions.

It seems that the most effective method of fighting with MITB attacks is an out-of-band (OOB) transaction verification process. The methods analysis the transaction details, as received by the host, which is a bank, to the user, which is a customer over a channel other than the browser. This is mainly conducted through call to the client. OOB method is ideal for mass markets as it leverages devices already in the public domain, such as: Landline etc.

2.2.2 Threats to Server

False Programs. A virus is a program that can infect other programs by modifying them. Modification includes a copy of the virus program, which may infect other programs. Computer virus has similarity with biological virus, a biological virus infects the machinery responsible for the living cell to work and a computer virus carries in its instructional code the recipe for making perfect copies of it. The typical virus takes temporary control of the computer`s disk operating system. Then, whenever the infected computer comes into contact with an uninfected piece of software, a fresh copy of the virus passes into the new program. Thus, the infection can be spread from computer to computer by unsuspecting users who either swap disks or send programs to one another over a network. In a network environment the ability to access applications and system service on other computers provides a perfect way to replicate itself.

Network worm programs use network connections to spread from system to system. Once active within a system, a network worm can behave like a computer virus, bacterium, It can implant Trojan horse programs or perform any number of disruptive or destructive actions. To replicate itself, a network uses some sort of network vehicle. Some of its uses are Electronic mail facility, Remote execution capability, and remote login capability. A worm mails a copy of itself to other systems via electronic mail facility (Wawrzyniak 2002). A worm executes a copy of itself on to a remote system as a user and then uses commands to copy itself from one system to the other. Then new copy of the program is then run on the remote system where, in addition to any functions that it performs at that system, it continues to spread in the same fashion. A network worm exhibits the same characteristics as a computer virus. A dormant phase, a propagation phase, a triggering phase, and an execution phase. The propagation phase generally performs the following functions, Searches for other systems to infect by examining host tables or similar repositories of remote system addresses. It establishes a connection with a remote system. Copies itself to the remote system and causes the copy to be run.

A logic bomb is a program, which lies dormant until a specific piece of program logic is activated. The most common activator for a logic bomb is a date. The logic bomb checks the system date and does nothing until a certain date. After that, the logic bomb activates and executes its code. A logic bomb could also be programmed to wait for a certain message from the programmer. The logic bomb could, for example, check a web site once a week for a certain message. When the logic bomb sees that message, or when the logic bomb *stops* seeing that message, it activates and executes its code. A logic bomb can also be programmed to activate on a wide variety of other variables, such as when a database grows past a certain size or a user’s home directory is deleted.

The most dangerous form of the logic bomb is a logic bomb that activates when something *does not* happen, for example: if the user does not log to the system for a month the data in the system are deleted. Since a logic bomb does not replicate itself, it is very easy to write a logic bomb program. This also means that a logic bomb will not spread to unintended victims. In some cases, a logic bomb is the most usual threat, since a logic bomb has to be targeted for a specific victim. The classic use for a logic bomb is to ensure payment for software. If payment is not made by a certain date, the logic bomb activates and the software automatically deletes itself. A more malicious form of that logic bomb would also delete other data on the system.

Backdoors are one of the most dangerous applications since usually computer user is not aware of their existence in the program or hardware device. In addition, backdoors usually permit to make use of the software or hardware with the most elevated privileges such as root or administrator.

As malicious code found in a virus or a Trojan horse normally lacks that most privileged account characteristic they are not considered backdoors with the exception of root kits, invisible malware flying under the radar of the operating system and anti-virus program, which includes a backdoor including remote access. Moreover, by means of key logger malware a hacker may intercept the admin password, which later, in phase two of the attack permits the cybercriminal to create a backdoor of some sort.

It is recommend to include the topic in the service level agreement, whereas due care is needed in all other cases. This includes, but is not limited to restricting disgruntled staff or employees who have been given notice from creating accounts with admin rights to the mandatory, updated antivirus on a patched system. Technically, an intrusion prevention and detection system can be helpful against backdoors, and all efforts against backdoors can be leveraged with IT security audits of course.

Threats to client in electronic banking transactions, the Internet is the medium of communication and www web pages is the interface. Since there is relatively high number of

mistakes in the security processes and the imperfection of the mechanisms used in the processes it is necessary to take look on the subjects, such as:
Web Pages Certificates - clients tend to not put enough attention to the certificates of web pages. Before each logging to the system it is necessary that the client has to check if the certificate of the web page is not false. In order to check it, the user has to click on the padlock located in the bar with the web page address. The certificate has to be issued by trusted certification authority.

Browser Behaviour - about the fact that the connection is encrypted the user is informed when there is a special icon on the taskbar of the browser and in the space for the web page address instead of usual prefix http:// there is https://. Moreover, if there is no padlock next to the web page address it is recommended to break the connection immediately and do not enter any confidential data.

Electronic Mail. It is recommended that users should always to log to the banks through bank's home page, it is highly dangerous to log through web page addresses sent by unreliable users. Usually such links are crafted and they connect with false web pages. False web pages are similar to the layout of bank's web pages, usually with slightly different address of the page. Through these process users are exposed to *phishing* and the aim of it is to swindle personal data, the number of credit card, user name or passwords from the client that is not aware of it. Usually the process concerns Internet banks, service to electronic payments or auction systems.

Venue of Logging. Clients should log to the systems mainly from their apartments or other places that are safe. It would not be a good idea to log to the bank from public places. In this case, the probability of interception of ID data necessary for the transactions is very high. Users that do not use their own computers cannot be sure that there are no viruses or Trojan horses that is impersonating for the browser or spying program that is able to copy the signs entered on the keyboard. Other possible danger is the imperfection of SSL protocol. The transaction as such s quite well protected, but during the connection it is possible to conduct the attack of man-in-the-middle. With the use of DNS service the theft is able to redirect the transmission with the bank to its own computer and after this connects it with the proper destiny. In the entire process, the answers from the bank are sent to the attacker's computer and after this to the appropriate client. The main problem covers the fact that client's browsers settle the parameters of the transaction not with the bank's server but with the cracksman. Consequently, he is able to read the entire transmission.
Displayed Messages - when the client is logging to his or her account it is very important to observe all messages displayed by the browser. In the situation discussed above, probable the browser displayed the message regarding faulty certificate; however, most of users usually click "OK" in order to continue work.

2.2.3 Transaction Threats

Generally speaking threats connected with electronic banking transactions can be divided into two groups: those connected directly with the bank and those, which appear outside the bank. The division of threats occurring in so-called remote transactions is presented in Table 1. The counteracts should be divided between both parties.

Table 1. Division of Treats Connected with Transactions

BANK	CLIENT
1. The elimination of the possibilities of byways of banking systems; 2. The protection of confidentiality of sets of encrypted passwords; 3. The protection of confidentiality of one time passwords; 4. The protection of integrity of computer operations; 5. The protection of integrity of logs.	1. The protection of confidentiality of passwords, including also one time passwords; 2. Antivirus protection; 3. The limitation regarding the access to the computer; 4. The protection of wireless access to the computer.

The necessity to provide electronic banking safety becomes more and more important as banks use more and more advanced information technology systems, which are created by the network of many different terminals characterized by huge differentiation of geographic location. Insufficient protection of those systems can result in the artificial banking liabilities, additional clients' liabilities and direct losses. Consequently, it seems that authorization is a basic tool in electronic IT systems. The applications of procedures that authorize, introduce to the computer system the control of the access to the resources on different organizational levels and it eliminates the threats of unauthorized access to resources of information technology systems.

3. Conclusions

Concluding, Poland can be perceived as an equal player on the international market of Internet banking service. The offer of the banks is very diversified, but methods of security are similar. Consequently, the security level is very similar. It is important to mention that security does not only depend on banks, which are not able to prevent some of the false transactions. Clients should also be on guard and carefully observe the behaviour of the service.

References

[1] Bakalarczyk S., 2012, Sustainable Enterprises - Methods of Security in Polish Electronic Banking Systems in Risk Minimizing [in:] Sustainable Enterprise of the Future, ed. by I. Hejduk, W. Grudzewski. Robert Morris University and Chodkowska University, Pittsburgh-Warsaw, p. 7-37.

[2] Bono S. et al., 2005, Security Analysis of a Cryptographically-Enabled RFID Device. USENIX Security Symposium.

[3] Connolly K., 2003, Law of Internet Security and Privacy. Aspen Publishers, New York, p. 30-32.

[4] Denning D.E., 1992, Kryptografia i ochrona danych, WNT, Warszawa, p. 230-235.

[5] Gantz J. et al., 2007, Pirates of the Digital Millennium, Upper Saddle River, Prentice Hall, p. 120-121.

[6] Jaźwiński J., Ważyńska-Fiok K., 1993, Bezpieczeństwo systemów, Wydawnictwo PWN, Warszawa, p. 100-105.

[7] Leyden J., 2003, Help! My Belkin router is spamming me, The Register.

[8] Stallings W., 1997, Ochrona danych w sieci i intersieci w teorii i praktyce, WNT, Warszawa, p. 33-35.

[9] Wawrzyniak D., 2002, Zarządzanie bezpieczeństwem systemów informatycznych w bankowości, Biblioteka Menadżera i Bankowca, Warszawa, p. 62-64.

[10] Wojciechowska - Filipek S., 2010, Technologia informacyjna w usługach bankowości elektronicznej, Difin, Warszawa, p. 23.