Proceedings of the 10th International Conference "Reliability and Statistics in Transportation and Communication" (RelStat'10), 20–23 October 2010, Riga, Latvia, p. 297-305. ISBN 978-9984-818-34-4
Transport and Telecommunication Institute, Lomonosova 1, LV-1019, Riga, Latvia

SECURITY REQUIREMENTS AND POSSIBILITIES OF RISK EVALUATION IN E-FINANCIAL PAYMENT SYSTEMS

Dalė Dzemydienė, Ramutė Naujikienė, Marius Kalinauskas

Department of Informatics and Software Systems
Mykolas Romeris University
Ateities 20, Vilnius, LT-08303, Lithuania
E-mail: daledz@mruni.eu, riman@mruni.eu, m.kalinauskas@mruni.eu

This paper analyses security requirements which can help to ensure the development of new security measures in e-payment operations. E-banking systems provide fast, reasonably secure and relatively low-cost service operations. Payment for goods and services using e-instruments is increasing. However, there is an increasing risk of possible breaches of security. Security support systems; authenticity, authorization, confidentiality, control, auditing, integrity, and minimal benefits for e-payment must be designed and applied according to security requirements and standards which need to be continually updated and improved. The European Union focuses on data protection for physical and juridical persons in order to keep e-services secure and discreet. EU legislation which determines financial payments involving data and information security standards and criteria is important for all EU member countries. E-banking systems ensure a prompt and adequate performance of safe financial transactions. Statistical data are analysed in order to evaluate how virtual currency transfers and payments for goods and services using e-instruments are increasing on a large scale. The technological development of e-payments increase the possibilities of quick and accurate transfers, however, cyber-security requirements and their implementation technologies have a great responsibility. Despite all the current security measures, threats to the security of e-payments are real and very serious. System 'cracking' tools and techniques are no less technologically advanced than their countermeasures. Most developed countries around the world pay a lot of attention to 'sensitive' information security. One of the categories of this kind of information is financial data. Some procedures are analysed through which software and hardware measures can be used for retrieving personal data by falsifying e-payment instruments, misleading the users of financial systems and thereby directing them onto dangerous content websites.

Keywords: *information communication technology, electronic financial payment (e-FP) system, e-safety, risk evaluation, e-security requirements, cybercrimes*

1. Introduction

This study focuses on the risk factors when assessing safety measures for e-financial payments. The development of information communication technologies (ICT) and the expansion of information systems allow increased usage of electronic payment methods. The development of information technologies has extended settlement options, therefore security requirements and their implementation technologies have acquired greater importance. Digital information can be easily disturbed and violated according to the adversely supported means, some of the unsafe factors and digitally processed information properties [1, 14]. The use of e-methods for financial transactions is gradually changing the perception of approaches and measures used in financial operations [2, 6, 17, 20]. According to the Lithuanian Information Society development strategy for 2009-2015, e-service usage is forecast to increase by up to 40%-60% until 2015 in business and in the public and state administrative sectors,

Networking allows different kinds of access, which can be positive or negative in terms of data security [14, 15, 16]. Increasing opportunities for consumers to use the web and the increasing size and importance of computer networks have had an influence on the appearance of different types of vulnerable transactions [9, 16, 21]. Since many entry points and different layers of information transmitters have been introduced into operations [8], security methods are not always able to control the security of the users' actions. E-banking operations and client sites require more complex defense means against web-based identity fraud, information violation, etc. [3, 14].

EU directives and regulations applicable in all the EU member states should be based on e-financial payment security, and each company, institution or organization should establish appropriate new security technologies that meet these standards and instructions (e.g, C(2010)593 final Commission Decision, 2010) [4]. The basic personal data protection legislation acts (Directive 95/46/EC, Directive 2002/58/EC, Directive 2006/24/EC) regulate the protection of privacy and also regulate data-flow protection measures in different ICT sectors. Members of the European Standards Organization (ESO) have been invited to extend the data protection directive 95/46/EC in accordance with the safety standardization report. The ESO is also charged with looking at the products of other standardisation institutions such as the ISO/IEC JTC1/SC27 which

deals with safe identity management, identification processes and the like. In addition the ESO has been invited to develop standardisation for coding technology, focusing on the computer programming performance of computing systems and access to the abundant computer resources that ensure personal privacy in distributed systems, as well as in grid platforms [10, 12]. Special attention should be paid to the ISO standards in order to improve and review them, with particular attention paid to those which can have the greatest influence on information security management.

In accordance with the directives of e-governing, new security technologies are required to ensure the protection of personal data in the field of public administration e-services, as well as in e-financial payments and their development [6]. An insufficient level of security can be caused by a low transaction completion rate (compared with a simple transfer of information on the internet), a lack of privacy and anonymity, operational complexity, transaction cost, and small-scale calculation losses. With a view to reducing the risk of losing money or sensitive information due to an e-payment disturbance, integrated safety measures need to be implemented.

The aims of this research are concerned with evaluating the situation of the usage of e-payments systems. The article discusses the risk factors when assessing safety measures in the areas of e-financial payments. Some uses of software and hardware in e-crime are reviewed, such as scanning personal information and falsification of e-payment instruments for deceiving users of e-financial payment systems.

2. Conceptual Representation of Safety Requirements in e-Financial Payment Systems

The major e-payment methods in e-banking systems are bank cards, e-checks, and e-money. Currently, one of the most common types of fraud is the use of fake bank cards. Counterfeit cards are made by using reliefs and imprints on a plastic card. Sometimes the cards are tampered with by coding them electronically. One electronic manipulation technique is directly related to the illegal retrieval of data from the electronic tracks on bank cards. A similar type of crime is often committed at the point of sale, when transaction data are copied using special equipment. Such crimes may also be committed by unauthorized interception of outgoing data or other means depending on data transfer methods (IBM Corporation, 2005).

According to the data of the Association of Lithuanian Banks, the total number of payment cards is increasing constantly (Fig. 1).

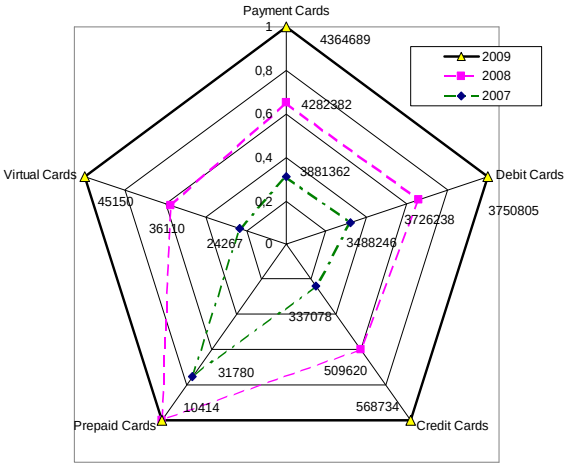


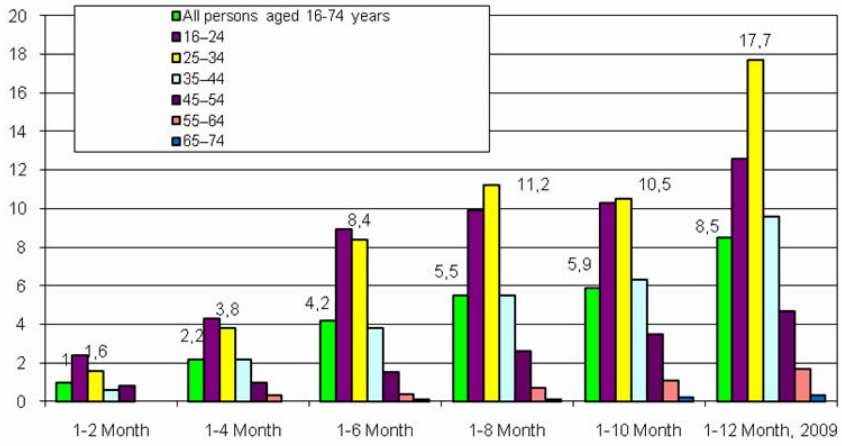
Figure 1. The distribution of usage different types of payment cards in Lithuania
(Data source: Association of Lithuanian banks, 2010)

For several years the number of virtual e-payment cards has been increasing also. So far these cards have a small share of the card market (1%), but these instruments of payment are valued for their security of transaction in electronic space. Virtual cards will take a greater share of the paying card market because of the processes related to the rising popularity of e-commerce. The total of individuals, who were using services related to e-commerce increased by 30.6% in the year 2009.

The EU average of goods and services purchased via the Internet was 28% in 2009. It is likely that the growing trend in the virtual card payments sector will increase, thus affecting the growth of fraud and the extent of the use of illegally acquired virtual payment data. A significant increase of registered

users of e-banking systems is an additional factor which leads to the conclusion that this sector is a potentially attractive target for criminal fraud.

Investments in banking systems security measures have reduced the risk of illegal actions against system users. New ICTs have expanded possible methods of e-security. Awareness of accident prevention has changed the situation of e-commerce. The number of users of e-commerce is increasing very rapidly. The changing patterns of usage of e-commerce services in different age groups in Lithuania during 2009 are illustrated in Fig. 2.



(Source: Data of Bank Association of Lithuania, 2010)

Figure 2. Illustration of the growing usage of e-commerce services during 2009 in Lithuania according to different aged groups

ICT technologies allow payment processes for various types of goods and services to be synchronized. Infrastructure for these kinds of actions is also under constant development. These factors explain the high increase in the popularity of e. payment instruments and methods.

Technical and software inaccuracies may lead to a weakening of protective programs and related data leakage. The security of e-financial payment systems is achieved via technological protection measures that support the safety requirements. These protect the confidentiality of personal and commercial information, and ensure protection against theft and the disclosure of important data (Fig. 3). Various measures are applied with a view to meet the clients' needs and to ensure the maximum security and reliability of these operations. However, no matter how technologically advanced the security system is, without the continuing application of new and more complex security measures it may still be vulnerable. The quality of electronic financial transactions is dependent on how the information is stored and who has the privilege to use it. The level of information technology security determines the appropriate level of information security assurance.

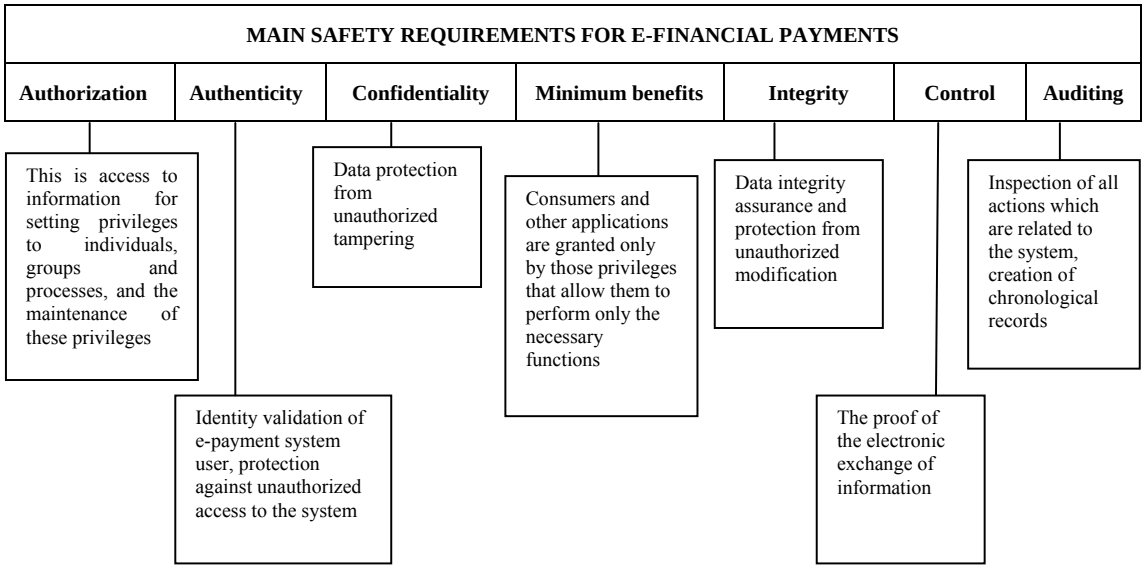


Figure 3. The main safety components in e-financial settlements

Security systems meant for supporting e-FP must be designed in accordance with safety requirements and standards. They are continually updated and improved, as the risk of fragility is possible [5]. Criminals make use of software errors (SW) or defensive gaps in the programs as well as of little-known computer networking software weaknesses. E-vulnerability is associated with the possibility of influencing information by e-means or other technologies (such an effect may weaken the protection programs and can allow access to the data). The act of processing data means that vulnerability could be due to the data transmission and processing properties, especially if staff skills are not sufficient in this area.

Information processing in computer systems is connected with the vulnerability of information and software usage as well as with the possibilities of invading through networking processes. Interoperable components of integrated databases are not protected fully. The vulnerability of data and information is one of the major components of information systems which require extreme safety software for online banking systems. In addition, safeguards bear the inherent characteristics of intelligent systems [3, 22, 7, 19].

Security is the key factor defining the quality of web services. Security areas include a number of web requirements. Secure Sockets Layer (SSL) is a technology which has become the marker standard that ensures secure data transmission via the Internet [19]. SSL was quickly recognized as a secure data transmission standard. The SSL protocol is used by most web browsers and server linkages because it can transfer data via the Internet very safely. The process of acquiring a secure SSL link connection, which ensures a secure communication between a web server and a client, is presented in Fig. 3.

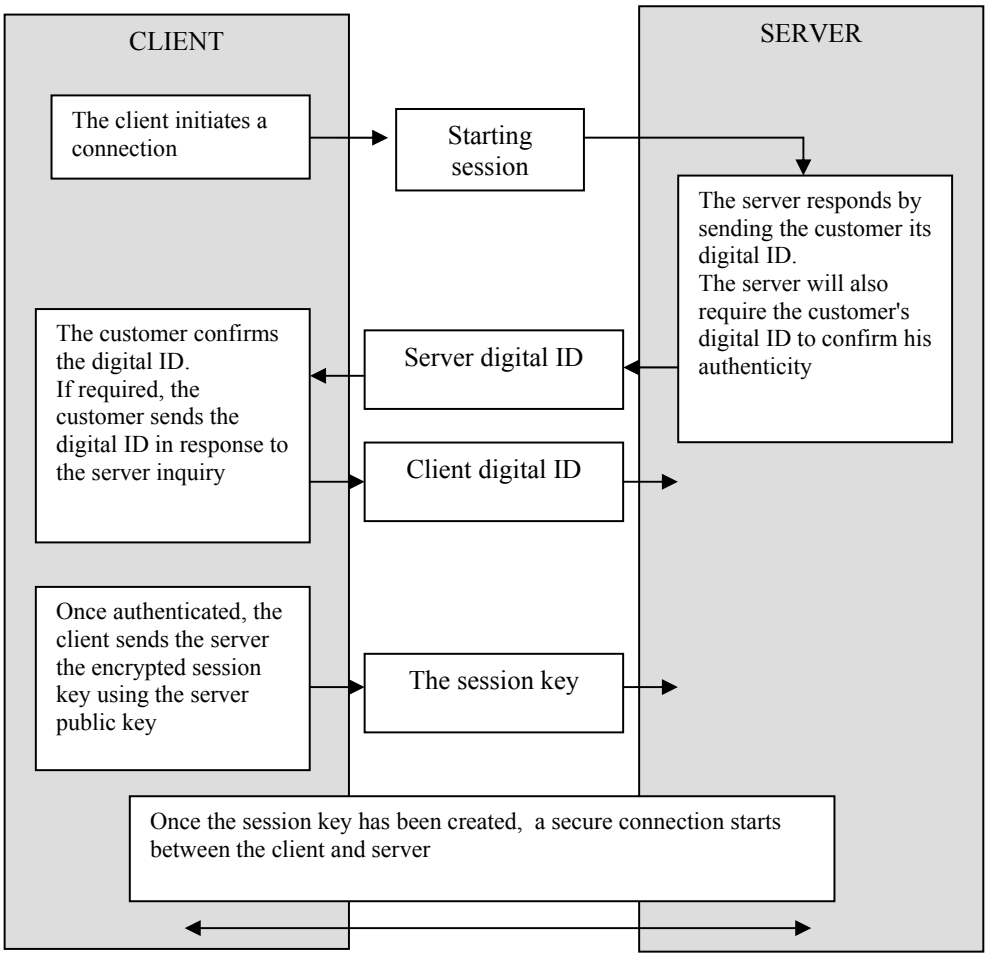


Figure 4. The principle scheme of SSL protocol for data transmission

SSL uses a public - private key encryption system. The SSL protocol requires the server to install a digital certificate. Usually a digital certificate consists of a public key owner, the owner of personal data, a validity period for the public key, the title of the organization that provides the digital certificate (CA)

designation, the serial number of the digital certificate, and a digital signature of the organization that provides the certificate.

The whole SSL certificate exchange takes place within a few seconds. The server confirms its authenticity via the internet browser's digital certificate, and checks whether the digital certificate has been received from the known Centre of Certificate Authority. The client must then be informed. At the same time, it is verified the validity period of the digital certification time has not expired [12, 13].

The Secure Hypertext Transfer Protocol (HTTPS) is preferred by the class of software links which support security. HTTPS includes communication protocols, and is used to transfer encrypted data via the Internet, which is based on the security layer protocol (SSL – Secure Socket Layer). HTTPS provides secure e-commercial transactions, for example online banking and other e-FP. Access to a secure server often requires a certain registration, login information and other necessary data [14, 15, 16]. A set of protocols and standards that can be used for exchanging data between applications and systems can be described in different programming languages. These applications can operate in different operating systems and use internet services for computer data interchange in networks.

The group of standards, indicating how to ensure the security of internet services is combined under the common name of WS-Security. These standards are not definitive, they are constantly being improved. This is only a small part of a family of standards known as WS. The ways of ensuring a certain level of security are an e-signature (issued by a certification services), personal identity cards, and the formation of closed user groups. WS-Transactions are a group of standards which ensure the reliable execution of transactions between business partners. The WS-Reliable Messaging standard ensures that messages reach the right contact in order and will not be duplicated. Simple Object Access Protocol (SOAP) is applied, for example, to forwarded messages. The WS-Security protocol describes SOAP messaging extensions, thus improving the quality of protection of the integrity, confidentiality, and authentication of each message. This mechanism may use a variety of security models and encryption technologies.

WS-Security also provides a general mechanism for bringing together artifacts and security items. WS-Security is also an extension mechanism that can be used for additional descriptions of authorizing characteristics contained in the message. This specification offers a number of SOAP extensions that can be used for the development of secure web services, ensuring integrity and confidentiality. WS-Security is quite flexible and is used as the basis of a wide range of security models, such as public key infrastructure (PKI), computer network authentication protocol (i.e. Kerberos) and SSL. WS-Security enables multiple security technologies, multiple trusted domains, signature formats and encryption technologies to other multiple security technologies. WS-Security has key enabling components that are used to interact with other internet service expansions and with the high-level requirements for specific protocols. These features allow the application of these standards to a wide range of security models and encryption technologies.

Security of e-financial payments depends on the security measures and means as a whole. The spectrum of potential data acquisition or intrusion into computer systems is quite broad. Appropriate use of security assurance measures makes it possible to protect important data and prevent criminal acts in e-space.

Table. 1. Dynamics of using different e-security means in financial payments applications of companies in Lithuania

Types of safety means	2005	2006	2007	2008	2009	2010
Total use of e-safety measures	79,0	82,5	83,9	88,3	92,1	90,4
Antivirus software	75	78,4	79,4	85,1	89,3	81,4
Software and hardware firewalls	26,4	29,9	32,9	37,4	42,7	42,7
Server Protection	19	24,4	25,5	31	36,7	39,8
Copy of data is not available to consumers	34,4	38,8	41,8	44,5	49	35
Data encryption for security reasons	8,6	9,9	10,4	17,2	18,7	20,3
Over the past year, faced with security problems	35,2	35,3	36,4	39,6	22,8	

The concentration of information and process frequency makes it possible to intercept data and modify or forward them in a short period of time at a great distance from the actual encroachment. The complexity of modern computer networks, the number of operations in networks and data processing techniques and levels lead to some uncertainty. Often even the creators of these networks cannot adequately control some of the processes performed in the networks.

The use of malware and other scams is becoming more frequent and more varied. In order to access web users who are potential targets, imitations of trusted web sites or well-known companies are used. A growing number of social networking users host their personal information on the Internet.

3. A Comparison of Usage of Electronic Financial Payment Means in Europe

E-payments are becoming one of the most widely used services. E-payment is likely to be affected by the growth of ICT usage and the popularity of e-services as a whole. An analysis of official statistical data shows the popularity of e-banking services and differentiations of usage among European countries (Eurostat, 2010; Dzemydiene, Naujikiene, 2008). The growth of usage of e-banking services is presented in Fig. 5, according to EU official data (Eurostat, 2010).

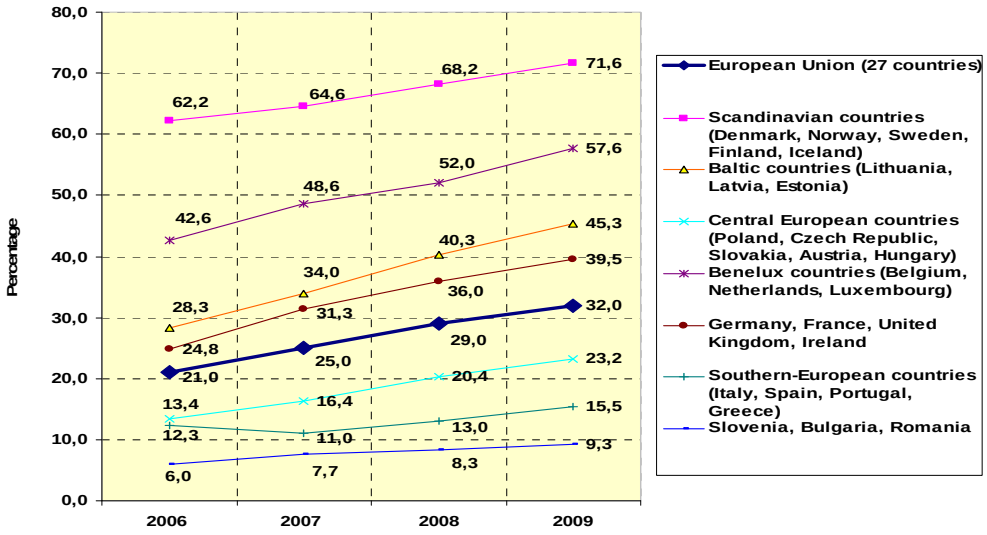


Figure 5. Increase in usage of e-banking services in European regions (Source: EU Statistical Office data, Eurostat, 2010)

Countries such as Germany, the United Kingdom, France, and Ireland are slightly ahead of the overall EU average in the context of e-banking usability. These countries have similar economic and social indicators, and therefore there is no significant difference in the prevalence of e-banking. Ireland may be regarded as a minor exception because its size, population, economic strength and potential cannot be equated to the United Kingdom, Germany or France. However, Ireland's investment in the e-financial sector is quite high, and therefore the level of use of e-banking services is significant despite the financial crisis. These countries use the most recent e-banking technological solutions and have populations with a high level of education who are willing and able to use these technologies. All these factors, as well as the requirement to adapt to the changing nature of e-banking and payment have led to the development and implementation of innovative e-banking methods and services.

These indicators may be related to cultural and technical aspects in the context of e-payment and e-banking services. The usage anofd need for technological solutions are positively related to income and other technological attributes and negatively related to socio-demographic factors such as living conditions and age.

From this point of view it is noted that the Scandinavian countries are the most advanced users of e-banking services. Scandanavian e-banking use is typically twice the EU average. The popularity of e-banking services may be a result of a well-developed banking sector in the Nordic region. Financial organizations also invest in web-based solutions and consistently introduce new methods and measures of e-payment to the consumers. The Scandinavians are among the leading purchasers of goods and services via the Internet in Europe. 59% of the Nordic region's population used these types of services in of 2009. It is not surprising that electronic forms of payment for goods and services are a near-universal

phenomenon in this part of Europe. Belgium, the Netherlands and Luxembourg have a high percentage of total population who use e-banking systems. This proportion was almost twice the EU average in 2009. However, according to e-banking services usability statistics, the EU average is 14% below that of the Scandinavian countries. Southern European countries are below the overall EU average.

The Baltic countries are ahead of the EU average in their usage of e-banking services. This is mostly the result of the widespread popularity of e-banking in Estonia. Usage of e-banking services in Lithuania and Latvia are at a similar scale, while usage Estonia is nearly approaching the level of the Scandinavian countries (Eurostat, 2010).

The continuing popularity of e-banking services is also raising new threats of illegal activities and actions (e-crimes). The conditions exist for increases in possible frauds or illegal attempts to steal financial property, personal data, and other significant information. One of the main qualities of e-payment is its complexity. These services are not limited to a single transaction or settlement method. Consequently, the range of possible illegal actions against these systems is quite wide.

The weakest links in the chain regarding e-banking services are the new member states of the EU (except Slovenia). The use of e-services in Romania and Bulgaria is low and is expected to remain unusually low for some years.

4. Evaluation of Financial Vulnerability and Potential Risk Factors in Electronic Payment Systems

The financial sector is very sensitive to any speculations, rumors or opinions connected with financial resources and data-related information. For this reason, security measures are designed primarily to ensure that the users of e-payment systems have no doubt about the reliability and security of information systems. The methods of encroachment on software or data by overcoming technical protection measures and data processing procedures are classified according to the object of attack; software changes and modification, illegal use of the data, and attempts on the data, including violations related to data that are regarded as a state, commercial or personal secrets. The methods of infringement of electronic payment are presented in Table 2, classifying them according to how these measures are realised.

Table 2. Possibilities to disturb safety in different layers of e-payment systems

Technical disturbance measures	Illegal software applications	Other illegal methods and measures
The use of fake ATMs	Key logger programs	Password thefts
Technical data collection tools made for network usage	Software code analysis tools (used for detecting security breaches)	Password guessing by using information about individuals
Bank card 'trap'	Web imitation for reliable Internet service providers	Analysis of security documentation inside the organization
Computer viruses causing damage to hardware	The use of virtual agents for illegal aims	Scanning data and software components for illegal operations
	Creation of computer viruses	

Security measures are needed for e-payment systems due to several factors. Security measures have been taken due to the frequency of e-crimes and their diversity in the e-FA, i.e., the disclosure of confidential information and personal data theft for personal gain.

Programs have been created for social network users that notify them about new messages and events. Persons engaged in e-crimes make use of this modern phenomenon through creating plug-ins and scripts that imitate social networking messages. After a user has chosen the 'safe' link, they are redirected to a web page with a harmful content. These types of site developer try not only to take advantage of the social networking services, but also try to discover popular keyword phrases by seeing which phrases are highest ranked in search engine query results. Thus they are attempts to increase the number of people who enter contaminated sites, and depending only on the objectives of the criminal activity, in order to perform harmful actions with a view to collecting personal data. Such data can be used in various fraudulent transactions.

5. Conclusions

New ICTs enable the development of new cyber security technologies. EU and Lithuanian legislation affect the safe use of e-financial settlement services in cyberspace. Safety support systems - the authenticity, authorization, confidentiality, control, auditing, integrity, and minimal benefits for e-EP must be designed in accordance with security requirements and standards, and they must be continually updated and improved. The development of e-payment options and the number of e-banking customers is steadily increasing. Online banking and e-banking systems provide fast, reasonably safe and relatively low-cost operations. Reimbursement for goods and services using electronic tools has become a important method of payments for goods and services. ICT development in this area is focused on people and business data confidentiality relating to the operations of e-FP, which largely means reducing the information security risks and possible vulnerabilities. Existing risk factors influence the development of e-payment security. The application of security standards and the implementation of modern ICT technologies increase the security of e-FP.

References

1. Angelopoulou, O., Thomas, P., Xynos, K., Tryfonas, T. 2007. Online ID theft techniques, investigation and response, *Int. J. Electronic Security and Digital Forensics*, Vol. 1, No. 1: 76-88.
2. Buračas, A. 2007. The competitiveness of the EU in context of the intellectual capital development. *Intellectual Economics.* 1(1): 19-28.
3. Business Guide: Guide of securing your e-government web site. Inspire official site [online]. 2010. Available from Internet: <http://www.verisign.com/static/005568.pdf>
4. C(2010)593 final Commission Decision of 5.2.2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. Brussels, 5.2. 2010
5. Client-side defence against web-based identity. Inspire official site [online]. 2010. Available from Internet: <http://www.isoc.org/isoc/conferences/ndss/04/proceedings/Papers/Chou.pdf >.
6. Dzemydienė, D., Naujikienė, R. 2008. Influence of e-banking systems on providing of e-public services. *Intellectual economics.* 2(4): 15-22.
7. Dzemydiene, D. 2010. Intelligence decision support systems for assistance in forensic investigation processes. In: Handbook of Electronic Security and Digital Forensics (Eds.) H. Jahankhani, D. Lilburn Watson, G. Me, F. Leonhardt. Publ. *World Scientific*. p. 603-630.
8. Dzemydienė, D., Dzindzalieta, R. 2009. Development of decision support system for risk evaluation of transportation of dangerous goods using mobile technologies. In: *Knowledge-based Technologies and OR Methodologies for Strategic Decisions of Sustainable Development*. (Eds). M. Grasserbauer, L. Sakalauskas, E.K. Zavadskas. V: Technika, p.108-113.
9. Dzemydienė, D., Naujikienė, R., Kalinauskas, M., Jasiūnas, E. 2010. Security requirements and risk assessment of electronic financial payments. *Technologijos mokslo darbai Vakarų Lietuvoje*. Vol. VII. Klaipėdos universiteto leidykla, p. 165-171 (in Lithuanian).
10. European Commission Enterprise and Industry Directorate – General: 2009 ICT Standardization Work Programme. Inspire official site [online]. 2010. Available from Internet: <http://portal.etsi.org/stfs/process/Forms/EC_2009_ICT_Standardisation_WP_v42.doc>.
11. Eurostat. Official European Commission statistics. Inspire official site [online]. 2010. Available from Internet: <http://epp.eurostat.ec.europa.eu/portal/page/portal/statistics/themes>.
12. IBM Corporation (2005) Technologies and Standards for Service-Oriented Architecture Project Implementation.
13. Instant SSL by Comodo: Know what HTTPS is and how SSL works. Inspire official site [online]. 2010. Available from Internet: <http://www.instantssl.com/ssl-certificate-products/https.html>.
14. Jahankhani, H. Al-Nemrat, A. (2010) Cybercrime. In: *Handbook of Electronic Security and Digital Forensics*. (Eds.) H. Jahankhani, D. Lilburn Watson, G. Me, F. Leonhardt. World Scientific Publishing Co. p. 573-583.
15. Kairaitis, K., Tamonis, M. (2007) Web Service Technology. In: *Proceedings of the Conference "Mokslas – Lietuvos ateitis*" (in Lithuanian).
16. Kiškis, M. (2009) Direct Electronic Marketing Opportunities for SMEs. *Intellectual Economics*. 2(6): pp. 61-72.
17. Martinaityte E. 2008. Globalization and financial markets size limits: credit risk management aspects. *Intellectual Economics.* 2(4): 52-58.

18. Statistics of the Association of Lithuanian Banks. Inspire official site [online]. 2010. Available from Internet: <http://www.lba.lt/go.php/lit/2009_m/1904>.
19. SSL Information Centre. Inspire official site [online]. 2010. Available from Internet: <http://www.verisign.com/ssl/ssl-information-center/index.html>.
20. Štitilis, D., Laurinaitis, M. 2008. Alternative payment systems: Lithuanian Outlook. *Intellectual Economics*. 2(4): 43-51.
21. Tryfonas, T. 2010. Information security management and standards of best practice. In: Handbook of Electronic Security and Digital Forensics. (Eds.) H. Jahankhani, D. Lilburn Watson, G. Me, F. Leonhardt. World Scientific Publishing Co. p. 207-236.
22. Zavadskas, E. K., Kaklauskas, A. 2009. Web-base decision support system for real estate. *Intellectual Economics*. 2(6): 51-60.