ISSN 1822-8011 (print)
ISSN 1822-8038 (online)
INTELEKTINĖ EKONOMIKA
INTELLECTUAL ECONOMICS
2010, No. 2(8), p. 21–29

EVALUATION OF SECURITY DISTURBANCE RISKS IN ELECTRONIC FINANCIAL PAYMENT SYSTEMS

Dalė DZEMYDIENĖ, Ramutė NAUJIKIENĖ, Marius KALINAUSKAS, Eugenijus JASIŪNAS

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

Abstract. The development of information and communication technologies (ICT) and the expansion of information systems encourage increased usage of electronic payment methods. Electronic banking systems provide fast, safe enough and relatively low-cost service operations. Reimbursement for goods and services using e-instruments is increasing. The paper analyzes new ICT which ensure the development of new security means in e-payment operations and the risk rising in possible security disturbances. Safety support systems—authenticity, authorization, confidentiality, control, auditing, integrity, and minimal benefits for e-payment—must be designed and applied according to the safety requirements and standards that must be always updated and improved. The European Union (EU) focuses on the protection of the data of natural and legal persons in order to keep e-services safe and sound. EU legal acts which determine the financial payment involving data and information security standards and criteria are important for all EU Member States. E-banking systems ensure a prompt and adequate performance of safe financial transactions. Statistical data are analyzed in order to evaluate the situation, i.e. to find out how virtual currency transfers and payments for goods and services using e-instruments are increasing on a large scale. Technological development of e-payment increases the possibilities of quick and qualitative transfers, but cyber-security requirements and their implementation technologies are essential issues to be considered. Despite all security measures, threats to the security of e-payments are real and very serious. Systems 'cracking' tools and techniques are no less technologically advanced than their countermeasures. Most developed countries around the world pay much attention to the security of 'sensitive' information. One of the categories of this kind of information is financial data. The article discusses risk factors in assessing safety measures for financial payment. The authors analyze some ways in which software and hardware measures can be used for retrieving personal data by falsifying e-payment instruments, misleading the users of financial systems and directing them to websites with dangerous content.

JEL Clasification: O7T; G10, G14, O10
Keywords: information communication technology, electronic financial payment (e-FP) system, e-safety, risk evaluation, e-security requirements, cybercrimes.
Reikšminiai žodžiai: informacinės komunikacinės technologijos, elektroninių finansinių atsiskaitymų sistema, e. sauga, rizikos vertinimas, e. saugumo reikalavimai, e. erdvės nusikaltimai.

1. Introduction

The development of information technologies extends settlement options; therefore, security requirements and their implementation technologies gain great importance. Computer information leads to the vulnerability of some of the factors and digitally processed information properties (Angelopuolos et al., 2007; Jahankhani and Al-Nemrat, 2010). Networking allows different kinds of access to the negative aspects in terms of data security (Kairaitis and Tumonis, 2007; Chou et al., 2010). Greater web consumer possibilities and increasing areas of computer networks influence the appearance of possible types of vulnerable actions (Tryfonas, 2010; Kiškis, 2009, Dzemydienė et al., 2010). Since many entry points and different layers of information transmitters are introduced into operations (Dzemydienė and

Dzindzalieta, 2009), those means are not always able to control the security of user's actions.

EU directives and regulations that are applicable in all EU Member States should be based on electronic financial payment (e-FP) security, and each company, institution or organization should establish appropriate new security technologies that meet the standards and instructions (for example, C(2010)593 final Commission Decision, 2010). The basic legislation for the protection of personal data (Directive 95/46/EC, Directive 2002/58/EC, Directive 2006/24/EC) regulates the protection of privacy and data-flow protection measures in different ICT sectors.

The members of the European Standards Organization (ESO) are invited to extend data protection Directive 95/46/EC in accordance with the safety standardization report. ESO are also invited to pay attention to other works of standardization institutions, such as the ISO/IEC JTC1/SC27, safe identity management, identification processes and the like. ESO are also invited to perform the coding technology standardization, focusing on the computer programming performance of computing systems and access to abundant computer resources that ensure personal privacy in distributed systems as well as in Grid platforms (ICT Standardization Work Program, 2009). Special attention should be focused on the ISO standards; by improving and reviewing them, particular attention should be paid to those standards 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 e-FP and its development. Insufficient level of security is influenced by low transaction completion rate (compared with a simple transfer of information on the Internet), lack of privacy and anonymity, operational complexity, transaction cost, small-scale calculation losses. With a view to reduce the e-payment disturbance risk to lose money or 'sensitive' information, the implementation of integrated safety measures are needed.

The authors of the article discuss risk factors in assessing safety measures in the areas of e-FP. The ways of software and hardware application in e-crimes (including scanning personal information, falsification of e-payment instruments for deceiving users of e-financial payment systems) are overviewed. The usage of e-methods for financial transactions is gradually changing the perception of approaches and measures of financial operations (Buračas, 2007; Štitilis and Laurinaitis, 2008; Martinaitytė, 2008; Dzemydienė and Naujikienė, 2008). Electronic service usage is forecasted to increase up to 40% until 2015 in business, public and state administrative sectors according to the Lithuanian Information Society Development Strategy for 2009–2015 (LR Government Resolution, 2008).

2. A Comparison of the Usage of Electronic Financial Payment Means in Europe

E-payments are becoming one of the most popular types of services which will be affected by the growth of ICT usage and the popularity of e-services on the whole. Official statistic data shows the popularity of e-banking services and differentiation of usage among the European countries (Eurostat, 2010; Dzemydienė and Naujikienė, 2008). Figure 1 shows the growth of the usage of e-banking services in European regions (Eurostat, 2010).

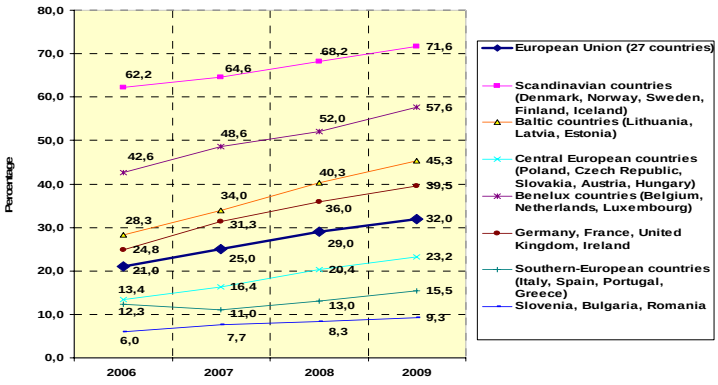

Figure 1. **Increase in the usage of e-banking services in the European regions,** according to the EU Statistical Office data (Eurostat,

It should be noted that the Scandinavian countries are the most advanced users of e-banking services. The average of the Scandinavian countries is two times upper the size of EU averageusage of e-bank services Scandinavians are obvious leaders in the field. 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. Scandinavians are among the first regarding the purchase of goods and services via the Internet in Europe. 59% of the population of the Nordic region used services of a similar nature in the year 2009. It is not surprising that electronic forms of payment for goods and services are a universal phenomenon in this European region. In Belgium, the Netherlands and Luxembourg, the percentage of the total population using e-banking systems is notably high—almost twice as large as the EU average (in 2009). However, according to e-banking services usability

statistics (in average), EU countries fall behind the Scandinavian countries by 14%.

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; therefore, the prevalence of e-banking differs insignificantly. 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, investment in to the e-financial sector in Ireland is rather high; thus, the level of the usage of e-banking services is significant despite the financial crisis. These countries use the most recent e-banking technological solutions and have a high level of educated population willing and able to use these technologies. All these factors as well as the necessity to adapt to the changing nature of e-banking and payment lead to the development and implementation of innovative e-banking methods and services.

Southern European countries fall behind the overall EU average of e-service popularity. These indicators may be related to cultural and technical aspects in the context of e-payment and e-banking services. The usage and the need for technological solutions are positively related to income and other technological attributes and negatively related to socio-demographic attributes such as the responsibilities and age of the inhabitants.

As a result of a significant Estonian contribution to widespread e-banking popularity among its population, the Baltic countries are ahead of the EU average in the usage of e-banking services. The levels of the usage of e-banking services in Lithuania and Latvia are similar, while Estonia is nearly approaching the Scandinavian countries (Eurostat, 2010).

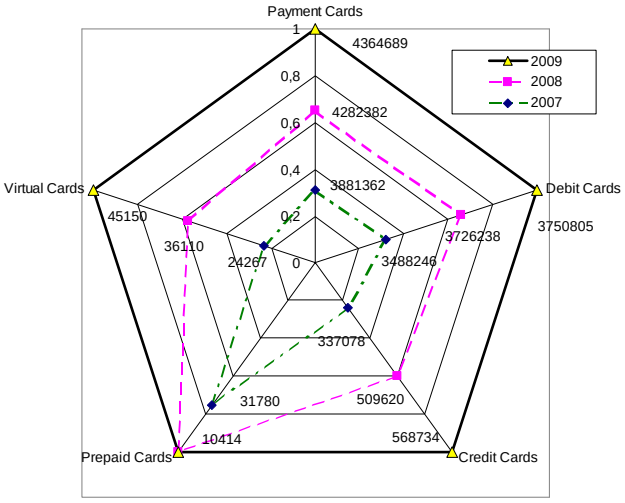

Figure 2. **Payment card distribution by type in Lithuania** (Source: Official data of the Association of Lithuanian Banks, 2010)

3. Financial Vulnerability and Potential Risk Factors in Electronic Payment Systems

The weakest links in the chain regarding e-banking services are the newcomers of the EU (except Slovenia). The indices of Romania and Bulgaria are rather poor; they are among the few European countries in which the usage of e-services remains low for several years in succession.

The continual popularity of e-banking services is raising new threats of illegal activities and actions. Possible frauds or illegal attempts to steal financial property, personal data and other significant information create the conditions for of an increase in e-crimes. One of the main qualities of e-payment is its complexity. These services are not limited to a single transaction or settlement method; therefore, the range of possible illegal actions against these systems is rather wide.

The complex of elements is applied in order to meet client needs and to ensure the maximum security and reliability of these operations. However, regardless of how technologically advanced the security system is, without constant appliance of new and more complex security measures it still may be vulnerable. The quality of electronic financial transactions depends on the way information is stored and the ones having the privilege to dispose it. The level of information technology security determines the appropriate levels of information security assurance.

The major e-payment methods in e-banking systems are bank cards, e-checks and e-money. Risk factors of each of these items are presented in Table 2. Despite the fact that the security measures of electronic payment systems are constantly improved, these systems may still be vulnerable due to unsafe methods of access to the system. Persons who have criminal intents do not need to connect to the system directly. After installing spyware or key logger on a user's computer, the offender can collect confidential information before the entrance into the system. Although this is not a problem of the e-banking system itself (because the source of the security breach is in a client's machine), it still corrupts the common reliability and credibility level of e-payment systems.

Currently, one of the most common forms of fraud is the usage of fake bank cards. Counterfeit cards are made by using relief and imprints on a plastic card, sometimes by coding them electronically. One of the electronic manipulation techniques is directly related to illegal retrieval of data from the microchips of bank cards. A similar type of crime is often made 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 the data transfer methods (IBM Corporation, 2005).

According to the data of the Association of Lithuanian Banks, the overall count of payment cards is constantly increasing (Table 1).

Table 1. **The usage of payment card types in Lithuania**

Type of paying cards	2007	2008	2009
Overall count	3825.3	4235.9	4296.0
Local	6.9	0.0	0.0
International	3818.5	4235.9	4296.0
"Visa" system	2588.9	2783.8	2803.9
"Mastercard" system	1227.6	1430.4	1468.0
Pre-paid cards	31.8	10.4	0.0

(Source: Annual statistics of the Association of Lithuanian Banks, 2009)

For several years the count of virtual e-payment cards has been increasing as well. So far, they have a small card market share (1%), but these paying instruments are valued for the security of transaction in the electronic space. Virtual cards are to take a greater share of the paying card market because of the processes related to the rising popularity of e-commerce. In 2009, the count of individuals who used services related to e-commerce increased by 30.6%. The EU average of purchasing goods and services via the Internet in 2009 is 28%. These trends in the sector of virtual card payments are likely to increase, thus affecting the growth of fraud and the extent of the use of illegally acquired virtual payment data. A significant increase in registered users of e-banking systems (Figure 3) is also one of the factors leading to a conclusion that this sector is potentially attractive to schemers and frauds.

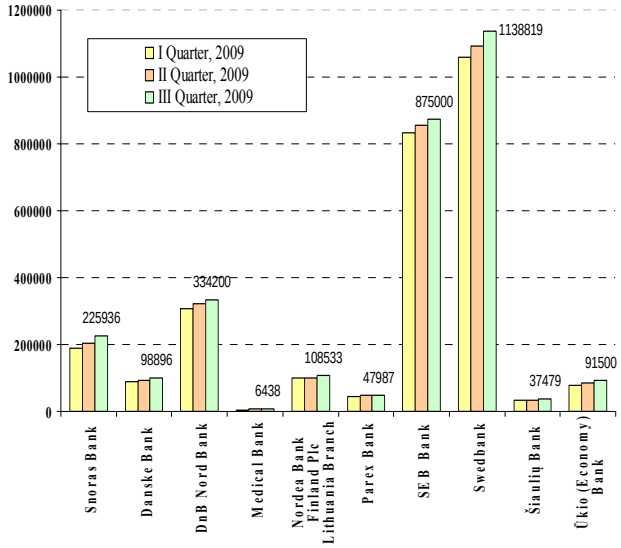

Figure 3. **The dynamics of the usage of registered clients in online banking systems of Lithuania in 2009**
(Source: Data of the Association of Lithuanian Banks, 2010)

Nevertheless, significant investments in banking systems security measures reduce the risk of illegal actions against the users. New ICT expand possible methods of electronic security. These technologies allow synchronizing payment processes for various types of goods and services. The infrastructure for these kinds of actions is also under constant development; therefore, the popularity of e-payment instruments and methods shows high increase rates.

Security measures are necessary for e-payment systems due to several factors. The financial sector is very sensitive to any 'speculations, rumours' and any opinions in connection with financial resources and data-related information. For this reason, security measures are designed primarily to ensure the reliability and security of information systems. Security measures have been taken due to frequent e-crimes and their diversity in e-FP systems, i.e. the disclosure of confidential information and personal data theft for personal gain.

The ways of software or data intrusion by overcoming technical protection and data processing procedures are classified according to the object of attack: software changes and modification, illegal use of data, attempts on the data including violations related to data that are regarded as a state, commercial or personal secret. Classified infringements regarding e-payment are presented in Table 2 (the classification is based on the ways of the realization of measures).

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 guess by using information about individuals
Bank card 'trap'	Web imitation for reliable Internet service providers	Analysis of security documentation inside the organization
Hardware-damaging computer viruses	The use of virtual agents for illegal aims	Scanning data and software components for illegal operations
	Creation of computer viruses	

The security of e-FP 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 the e-space.

The use of malware and other scams becomes more frequent and the possible ways more varied. In order to target persons to those infected sites, names of well-known companies or trusted websites are used and their services are imitated. A growing number of social networking users put their personal information on the Internet. Programs to notify them about new messages and events are created. Persons engaged in e-crimes make use of this phenomenon; they create plug-ins and scripts that imitate social networking messages. After a user has followed the 'safe' link, he is redirected to a web page with dangerous content. These types of site developers try to maximize not only social networking services, but also popular keyword phrases in order to increase their ranking in the search for engine query results. Thus, it is attempted to increase the number of people entering the contaminated sites and perform harmful actions with a view to collect personal data. Such data can be used in various fraudulent transactions.

4. Comprehension of Safety Requirements and their Integrated Implementation in Electronic Payment Operations

Information processing in computer systems is connected with the vulnerability of information and software usage as well as with the possibilities to invade through networking processes. Interoperable components of integrated databases are not fully protected. The vulnerability of data and information is one of the major components of information systems that require extreme safety software for online banking systems. In addition, safeguards bear inherent characteristics of intelligent systems (Business Guide, 2009; Zavadskas and Kaklauskas, 2009; Dzemydiene et al., 2010; Tryfonas, 2010).

Technical and software inaccuracies may lead to a weakening of the protective programs and data leakage. The security of e-FP systems is achieved via technological protection measures that support the safety requirements. They are meant for maintaining the confidentiality of information regarding private persons or businesses, ensuring the protection against theft and disclosure of important data (Figure 4). Security systems meant for supporting e-FP must be designed following the safety requirements and standards; they are always updated and improved, as the risk of fragility is possible (Chou et al., 2010).

Concentration of information and process frequency makes it possible to take over the data, modify or forward them with an ample distance from the encroachment object over a short period of time. The complexity of modern computer networks, the number of operations in networks as well as data processing techniques can cause some uncertainties, often even the creators of these networks cannot adequately control the main processes performed in the network.

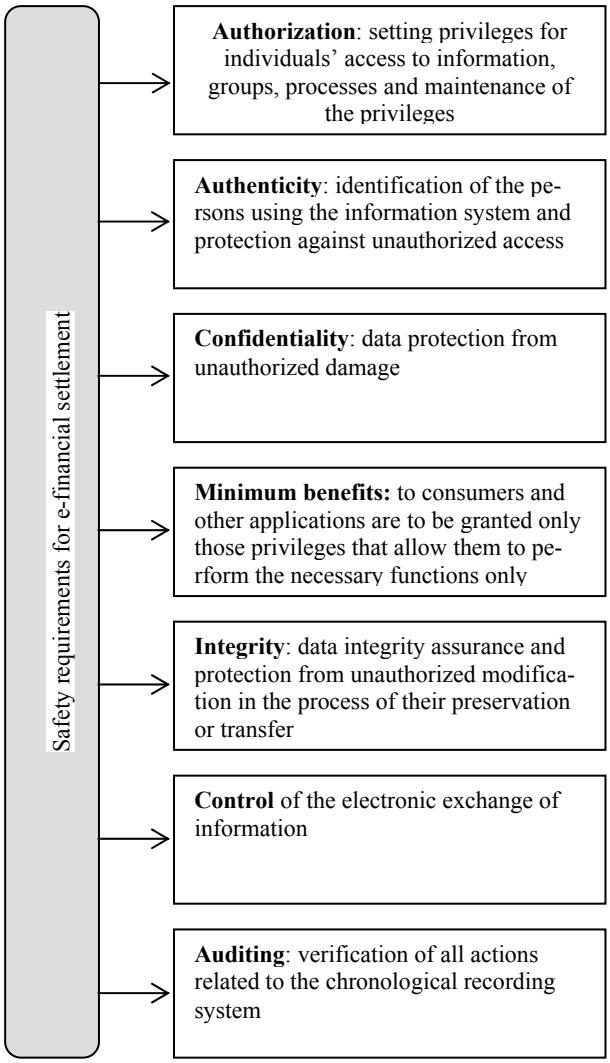

Figure 4. **The main safety components in e-financial settlements**

Criminals make use of software errors or defensive gaps in the programs as well as little-known computer networking software weaknesses. E-vulnerability is associated with the possibility of information influence by e-means or other technologies (such an effect may weaken the protection programs and allow access to the data). The vulnerability of data processing process means is a result of insufficient skills and competence of the staff regarding data transmission and processing properties.

4.1. Examples of electronic payment protection components

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 became the marker standard that ensures secure data transmission via the Internet. 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. 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, validity period of the public key, the title of 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 (Figure 5).

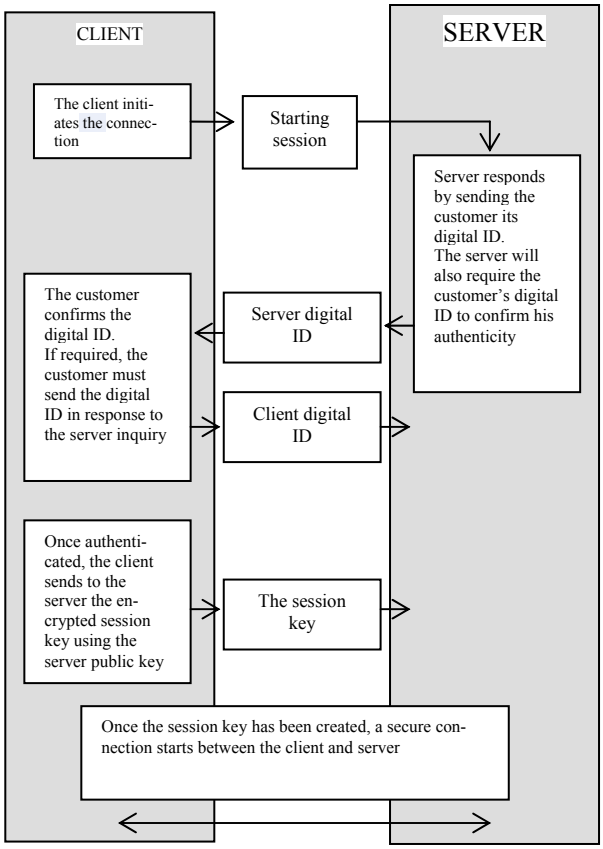

Figure 5. **The principle scheme of SSL protocol for data transmission**

The process of getting a secure SSL link connection which ensures a secure communication between a web server and the client is presented in Figure 5. The whole SSL certificate exchange lasts for a few seconds. The server confirms its authenticity by the Internet browser's digital certificate and checks whether the digital certificate is received from the known Centre of Certificate Authority. The client must be informed and, at the same time, it is checked whether the digital certification time has not expired (IBM, 2005; Instant SSL by Comodo, 2010).

4.2. Integrated web services security components

The Secure Hypertext Transfer Protocol (HTTPS) is preferable to the class of software links which support security. HTTPS include communication protocols and is used to transfer encrypted data via the Internet, which is based on the security layer protocol (SSL). 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 (Jahankhani and Al-Nemrat, 2010; Kairaitis and Tamonis, 2007; Kiškis, 2009). A set of protocols and standards can be used for the exchange of 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 web service security (WS-Security). These standards are not definitive, they are constantly improved. This is only a small part of the family of standards known as WS-Security.

The ways of ensuring a certain level of security are:

- an e-signature issued during the certification services;
- personal identity cards;
- the formation of closed user groups.

WS-Transactions are the group of standards meant to ensure reliable execution of transactions between business partners. WS-Reliable Messaging standard ensures that messages reach the right contact order and will not be duplicated. Simple Object Access Protocol (SOAP) is applied, for example, to forward messages. WS-Security protocol describes SOAP messaging extensions, thus improving the quality of protection through message 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 artefacts and security items. WS-Security is also an extension mechanism that can be used to the further description 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 main design of a wide range of security models, such as public key infrastructure (PKI), computer network authentication protocol (e.g. 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 the 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 for a wide range of security models and encryption technologies.

Conclusions

The development of e-payment options and the numbers of e-banking customers is steadily increasing. Online banking and e-banking systems provide fast, safe enough and relatively low-cost operations. Reimbursement for goods and services using electronic tools becomes a noticeable part of payments for goods and services. New ICT enable the development of new cyber security technologies. The EU and the Lithuanian legislations affect the safe use of e-financial settlement services in cyberspace. Safety support systems—authenticity, authorization, confidentiality, control, auditing, integrity for e-EP are designed following the safety requirements and standards, and they must be always updated and improved. ICT development in this area is focused on people and business data confidentiality relating to the operations of e-FP, in order to reduce information security risks and possibilities of vulnerability. The existing risk factors influence e-payment security development and 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. *International Journal of Electronic Security and Digital Forensics*, 1(1): 76-88.
2. Association of Lithuanian Banks [accessed 30-04-10]. <http://www.lba.lt/go.php/lit/2009_m/1904>.
3. Buračas, A. (2007). The competitiveness of the EU in the context of intellectual capital development. *Intellectual Economics.* 1(1): 19-28.
4. C(2010)593 final Commission Decision of 5 February 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 February 2010.
5. Chou, N. et al. (2010). *Client-side Defense Against Web-based Identity Theft*. ISOC [accessed 20-03-10]. http://www.isoc.org/isoc/confeences/ndss/-04/proceedings/Papers/-Chou.pf >.
6. Dzemydienė, D.; Naujikienė, R. (2008). Influence of e-banking systems on the provision of e-public services. *Intellectual economics,* 2(4): 15-22.
7. Dzemydienė, D. (2010). Intelligence decision support systems for assistance in forensic investigation processes. In H. Jahankhani, D. Lilburn Watson, G. Me and F. Leonhardt (eds), *Handbook of Electronic Security and Digital Forensics*. World Scientific Publishing Co, 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 M. Grasserbauer, L. Sakalauskas, and E. K. Zavadskas (eds), *Knowledge-based Technologies and OR Methodologies for Strategic Decisions of Sustainable Development*. Vilnius: Technika, 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*. vii. Klaipėda: Klaipėdos Universiteto leidykla, 165-171.
10. European Commission Enterprise and Industry Directorate-General (2010). *2009 ICT Standardization Work Programme* [accessed 10-05-10]. <http://portal.etsi.org/stfs/process/Forms/EC_2009_ICT_Standardisation_WP_v42.doc>.
11. Eurostat. Official European Commission statistics [accessed 10-05-10]. <http://epp.eurostat.-ec.europa.euportal/page/portal/statistics/theme>.
12. IBM Corporation (2005). *Technologies and Standards for Service-oriented Architecture Project Implementation* [accessed 10-05-10]. <http://-www.ibm.com/us/en/>.
13. Instant SSL by Comodo (2010) [accessed 10-05-09]. <http://www.instantssl.com/sslcertificateproducts/https.html>.
14. Jahankhani, H.; Al-Nemrat, A. (2010). Cybercrime. In H. Jahankhani, D. Lilburn Watson, G. Me and F. Leonhardt (Eds), *Handbook of Electronic Security and Digital Forensics*. World Scientific Publishing Co, 573-583.
15. Kairaitis, K.; Tamonis, M. (2007). Web Service Technology. *Proceedings of the Conference 'Mokslas – Lietuvos ateitis'*, 29-30 March 2007, Vilnius.
16. Kiškis, M. (2009). Direct electronic marketing opportunities for SMEs. *Intellectual Economics*, 2(6): 61-72.
17. LR Government Resolution (2008). 'On the Project of the Lithuanian Information Society Development Strategy for 2009–2015'.
18. Martinaitytė, E. (2008). Globalization and financial markets size limits: credit risk management aspects. *Intellectual Economics,* 2(4): 52-58.
19. SSL Information Centre [accessed 05-09-09]. <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 H. Jahankhani, D. Lilburn Watson, G. Me and F. Leonhardt (eds), *Handbook of Electronic Security and Digital Forensics*. World Scientific Publishing Co, 207-236.
22. Verisign (2010). *Business Guide: Guide to Securing Your E-Government Web Site* [accessed 03-08-10]. <http://www.verisign.com/static/005568.pdf>.
23. Zavadskas, E. K.; Kaklauskas, A. (2009). Web-based decision support system for real estate. *Intellectual Economics*, 2(6): 51-60.

SAUGOS PAŽEIDIMŲ RIZIKOS VERTINIMAS ELEKTRONINIUOSE FINANSINIUOSE ATSISKAITYMUOSE

Dalė DZEMYDIENĖ, Ramutė NAUJIKIENĖ, Marius KALINAUSKAS, Eugenijus JASIŪNAS
Mykolo Romerio universitetas, Lietuva

Santrauka. Elektroninės bankininkystės sistemos užtikrina greitą bei pakankamai saugų transakcijų atlikimą finansiniuose atsiskaitymuose. Europos Sąjungos teisės aktai, apibrėžiantys finansiniuose atsiskaitymuose naudojamų duomenų ir informacijos saugumo kriterijus ir standartus, yra svarbūs visoms ES šalims narėms. Virtualūs valiutų pervedimai bei atsiskaitymai už prekes ir paslaugas, naudojant elektroninius instrumentus, įgyja vis didesnį mastą. Nepaisant to, grėsmės elektroninių atsiskaitymų saugumui yra realios ir labai rimtos. Sistemų „nulaužimo“ įrankiai bei metodai technologiškai beveik tokie pat pažangūs kaip ir apsaugos priemonės. Labiausiai išsivysčiusios pasaulio šalys daug dėmesio skiria „jautrios“ informacijos saugumui. Prie tokios informacijos kategorijos priskirtini su finansinių atsiskaitymų operacijomis susiję fizinių bei juridinių asmenų duomenys. Straipsnyje nagrinėjami rizikos veiksniai vertinant saugos reikalavimų priemones finansiniuose atsiskaitymuose. Analizuojami kai kurie būdai, kaip elektroniniams nusikaltimams sukurtą programinę bei techninę įrangą galima panaudoti nuskaitant asmens duomenis, klastojant elektroninio mokėjimo instrumentus, klaidinant elektroninių finansinių sistemų naudotojus.

Dalė Dzemydienė is a Professor Habil. Dr., the head of the Department of Informatics and Software Programs of the Faculty of Social Informatics of Mykolas Romeris University (Lithuania). She has a Diploma with Honour in Applied Mathematics, the specialization of software engineering (1980). She was awarded the degree of Doctor of Philosophy in Mathematics–Informatics (1995), Habil. Dr. in Social Sciences (2004). She is the author of over 100 research articles, one monograph and four textbooks. She is the organizer of international conferences on information systems and database development. She is a member of the Lithuanian Computer Society (LIKS), the European Coordinating Committee for Artificial Intelligence (ECCAI) and the Lithuanian Operation Research Association. Research interests: artificial intelligence methods, knowledge representation and decision support systems, e-services, software systems and ICT development.

Dalė Dzemydienė – Mykolo Romerio universiteto Socialinės informatikos fakulteto Informatikos ir programų sistemų katedros vedėja, profesorė. 1980 m. Kauno technologijos universitete įgijo taikomosios matematikos specialybę, inžinieriaus matematiko programuotojo kvalifikaciją. 1995 m. apgynė matematikos-informatikos mokslų daktaro disertaciją, 2004 m. atliko socialinių mokslų vadybos ir administravimo srities habilitacijos procedūrą. LIKS, ECCAI, LitORS narė. Mokslinių interesų sritys: dirbtinio intelekto metodai, žinių vaizdavimas, sprendimų paramos sistemos, darnaus vystymosi procesų vadyba ir rizikos vertinimas, e. paslaugų vystymo metodai. Paskelbė daugiau kaip 100 mokslinių straipsnių, monografijos ir dviejų vadovėlių autorė.

Ramutė Naujikienė is a lecturer in the Department of Informatics and Software Programs of the Faculty of Social Informatics of Mykolas Romeris University (Lithuania). She has a Diploma in Physics Engineering, Vilnius University (1978). She is a member of the Lithuanian Computer Society (LIKS), ECDL instructor. She is the author of over 30 research articles, a co-author of three textbooks. Research interests: methods for information management systems development, e-services, evaluation of public administration e-services.

Ramutė Naujikienė – Mykolo Romerio universiteto Socialinės informatikos fakulteto Informatikos ir programų sistemų katedros lektorė. 1971 m. Vilniaus universitete įgijo inžinieriaus fiziko specialybę, kvalifikaciją kėlė programų sistemų ir duomenų bazių taikymo srityje. Mokslinių interesų sritys: informacijos vadyba, informacinės sistemos, duomenų bazės, viešųjų paslaugų vystymo metodai. Paskelbė daugiau kaip 30 mokslinių straipsnių, yra dviejų mokomųjų metodinių leidinių ir dviejų vadovėlių autorė.

Marius Kalinauskas is a lecturer in the Department of Informatics and Software Programs of the Faculty of Social Informatics of Mykolas Romeris University (Lithuania). He holds a Master's degree in Informatics Law (2009). Research interests: artificial intelligence and law, ICT, information management systems development, e-services.

Marius Kalinauskas – Mykolo Romerio universiteto Socialinės informatikos fakulteto Informatikos ir programų sistemų katedros lektorius. 2009 m. MRU įgijo teisės magistro kvalifikacinį laipsnį. Mokslinių interesų sritys: teisės informatika, intelektualizuotos informacinės sistemos, informacinės komunikacinės technologijos, e. nusikaltimų rizika, asmens duomenų teisinė apsauga.

Eugenijus Jasiūnas is a lecturer in the Department of Informatics and Software Programs of the Faculty of Social Informatics of Mykolas Romeris University (Lithuania). He is a member of the Lithuanian Computer Society (LIKS). Research interests: information management systems development, e-services, business driven information systems.

Eugenijus Jasiūnas – Mykolo Romerio universiteto Socialinės informatikos fakulteto Informatikos ir programų sistemų katedros lektorius. 1978 m. Vilniaus universitete įgijo taikomosios matematikos specialybę. Kvalifikaciją kėlė Profesinio tobulinimosi centre, Kauno technologijos universitete „Kokybės vadyba (ISO 9000 serijos standartai)“, o “Date Centrale” (Danija) – „Gyventojų registro projektavimo klausimai, asmens dokumentų projektavimo ir gamybos technologiniai ypatumai“ tema bei Erfurto duomenų apdorojimo centre (Vokietija) kolektyvinio naudojimosi skaičiavimo centro (KNSC) duomenų bazių projektavimo srityse. Mokslinių interesų sritys: duomenų bazės, informacijos vadyba, verslo informacinės technologijos, statistika.