Marta Juszczyk[1], **Marek Milosz**[2], **Elzbieta Milosz**[3]

VARIOUS METHODS FOR EMPLOYEES' AUTHENTICATION AT SMES

The paper presents the study results on the level of acceptance of different authentication methods in computer systems. The research was conducted among employees of small and medium-sized enterprises (SMEs). The research has demonstrated the ways of getting access to resources by the methods based on knowledge, special device and biometrical features. There is also an attempt to assess the actual state of using these methods in SMEs, readiness of employees for introduction of new methods, and predictions on their further implementation.

Keywords: *authentication method; new technologies; SMEs.*

Марта Ющик, Марек Мілош, Ельжбета Мілош

РІЗНІ МЕТОДИ АУТЕНТИФІКАЦІЇ СПІВРОБІТНИКІВ НА МАЛИХ ТА СЕРЕДНІХ ПІДПРИЄМСТВАХ

У статті представлено результати досліджень рівня сприйняття різних методів аутентифікації в комп'ютерних системах підприємств. Дослідження проводилося на співробітниках малих і середніх підприємств (МСП). Показано шляхи доступу до ресурсів за допомогою методів, заснованих на знаннях, на унікальному предметі – пристрої аутентифікації або за біометричними параметрами. Зроблено спробу оцінити використання цих методів в МСП, готовність співробітників до їх впровадження, а також перспективи їх подальшого застосування.

Ключові слова: *методи перевірки автентичності; нові технології; малі та середні підприємства.*

Рис. 8. Літ. 14.

Марта Ющик, Марек Милош, Эльжбета Милош

РАЗЛИЧНЫЕ МЕТОДЫ АУТЕНТИФИКАЦИИ СОТРУДНИКОВ НА МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЯХ

В статье представлены результаты исследований уровня принятия различных методов аутентификации в компьютерных системах предприятий. Исследование проводилось на сотрудниках малых и средних предприятий (МСП). Показаны пути доступа к ресурсам с помощью методов, основанных на знаниях, на уникальном предмете – устройстве аутентификации или по биометрическим параметрам. Сделана попытка оценить использование этих методов в МСП, готовность сотрудников к их внедрению, а также перспективы их дальнейшего использования.

Ключевые слова: *методы проверки подлинности; новейшие технологии; малые и средние предприятия.*

Introduction. Enterprises face many new challenges these days. They have to adjust their products, services or production methods to severe competition at markets, and look for new effective, flexible, and economically profitable innovations (Ran, 2013).

Granting access to resources only to authorized users is one of crucial factors of data protection at enterprises (Felker and Sacha, 2012). Usually access is gained in a three-step process (Ballad et al., 2010; Josang et al., 2005): user declares identity (identification), provides its proof (authentication), and is allowed the use of a desired resource or system (authorization).

[1] Lublin University of Technology, Poland.
[2] Lublin University of Technology, Poland.
[3] Lublin University of Technology, Poland.

There are 3 basic methods of authentication (Li, 2011; Windley, 2008). The first one is based on user's knowledge. It is usually typing a password or a secret shared with a system (e.g. previously fixed answer to a question). Other method requires using a thing recognized by the system like electronic card/USB device or token. The third way of authentication is providing some biometric features of a user like finger print, retina scan or voice (Modi, 2011). It also requires special equipment like a reader or scanner.

Application of a particular method now and in the future is a question of knowledge, funds, needs and decision-maker beliefs. What is the picture of small and medium enterprises (SMEs), where funds are limited and technical innovations introduced generally later? The previous research concerned large enterprises in Poland (Juszczyk, 2012).

Pros and cons of particular authentication methods. Passwords seems to be the most frequently used method, basically due to the fact, that it was the first way of access protection, and secondly, due to its simplicity, maturity (a password to programs/files is standard) and has no additional costs. Passwords, however, have some drawbacks: they can be relatively easily compromised by using one from a wide range of methods or they can be revealed to a third party (Burnett, 2005).

To deal with this challenge, and thus to increase the level of data protection, special devices have been introduced. They provide encrypted authentication data which cannot be recognized by humans (e.g., smart card) or one-time passwords (e.g., token OTP). The additional benefit of these devices is the possibility of other usage, e.g., for physical protection of enterprise resources (Cross, 2008). But this method does not protect against giving device to an unauthorized person. Moreover, it requires certain financial spending for purchasing and replacing devices for each user.

The latest, biometrical method (Kaur et al., 2014) highly reduces the risk of unauthorized access. To prove the claimed identity, personal features are scanned or read and compared with the reference pattern. But this method has some difficulties and dilemmas. Firstly, a user changes some characteristics (especially behavioral ones) during life, which can result in misidentification (Graham-Rowe, 2010). Secondly, in case of a compromised reference pattern, a user cannot change it like a password – it is a set of personal and sensitive data, and brings sometimes irreversible consequences to a particular person. Moreover, biometrical method requires devices to input biometrical data, which means additional, and so far, quite significance costs.

The research problem. Small and medium-sized enterprises, like large ones, need to protect their data. Previous studies (Milosz and Juszczyk, 2012) have shown that the level of information security in Polish SMEs is not sufficient. SMEs have limited funds for purchase, introduction and development techniques of granting access, but also for trainings of employees (Milosz and Juszczyk, 2012). How SMEs deal with this problem? Which solution is used and does it provide satisfactory level of data security? How the problem of data securing is perceived by employees?

The research hypothesises were formulated as follows:

H1. SMEs do not invest in different methods of granting access, but relay mostly on logins and passwords.

H2. Employees perceive the method used in their companies as safe.

H3. There are differences between the level of acceptance of authenticate methods.

H4. Employees are open to new solutions.

H5. There are differences between IT professionals and other employees in terms of preferable solutions.

The research method and its implementation. To complete the research the questionnaire method has been used. The questionnaire consisted of 3 parts:

- basic information about respondents and their enterprises,
- current solutions in enterprises,
- employees preferences.

The respondents were divided into two groups: employees whose main area of interest is IT (IT professionals or employees of IT company) and others.

Enterprises were divided into groups depending on the size: micro- (up to 9 employees), small (10–49 employees) and medium-sized enterprises (50–249 employees).

The research was conducted in December 2012 in Lublin region. The questionnaire was realized only on paper. The return was low, probably due to sensitive area of questions. Finally, only 65 questionnaires were collected.

Results. Among respondents, 43% were employees of microenterprises, 36% of small and 21% of medium-sized enterprises. 46% of the respondents were IT specialists or IT company employees.

85% of the respondents use passwords to secure access to computers, and 43% – also to applications. For 69% of the respondents it is the only method used. 18% of the respondents declare using a token or a smart card for authentication, and 9% – fingerprint reader. 6% of the respondents do not use any security access (Figure 1). Let us assume that enterprises base on low or no cost solutions (75% in total), thus confirming the hypothesis 1.

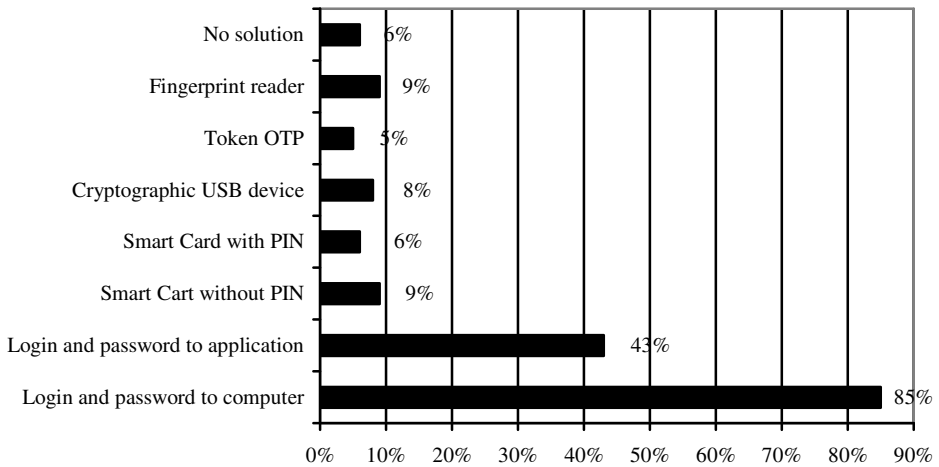

Figure 1. **Which solution do you use at work?,** *own research*

Surprisingly, only 40% of the respondents believe that their companies use a secure method of authentication, 20% of them perceive the used solution as insufficiently secure, and 40% describe it as insecure. It means that employees are aware of the threats related to the methods they use. This rejects the hypothesis 2. While examining the preferences on selecting the ideal solution, an interesting relationship was

revealed. Employees, who believe that solution used in their companies does not protect data, prefer more advanced method like based on tokens/smart cards or biometrical features (Figure 2).

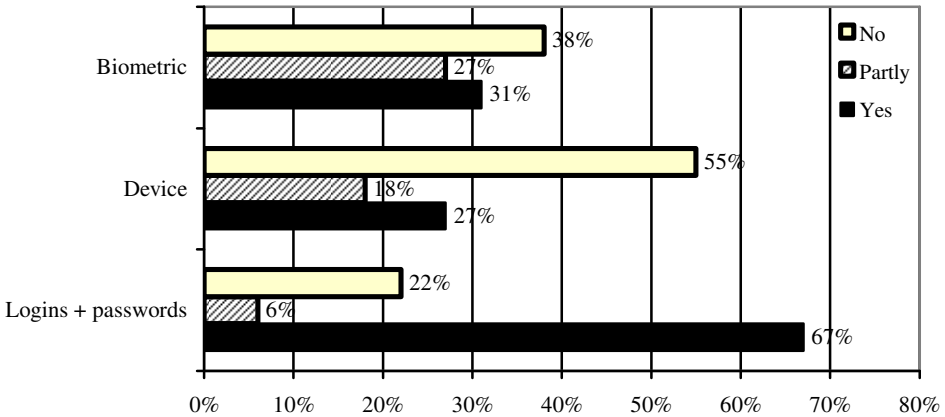

Figure 2. **Does your enterprise use a solution which you perceive as safe?,** *own research*

It leads us to some assumption. If employee notices that the used method is risky and endanger company's resources or employee's interests, he or she will be less resistant to new solutions. Thus, the situation emphasizes the role of education here.

Examination of the respondents' preferences revealed interesting facts (Figure 3). Passwords, the oldest and the most popular solution, are generally accepted – almost 70% of the respondents declared positive or enthusiastic attitude, but also it has the lowest rate of extreme opinions (enthusiastic and negative). On the other end is the authentication based on biometric features. It is rather accepted (35% positive and 17% enthusiastic), but also 14% of employees perceives it negatively.

Hypothesis 3 can be considered as confirmed.

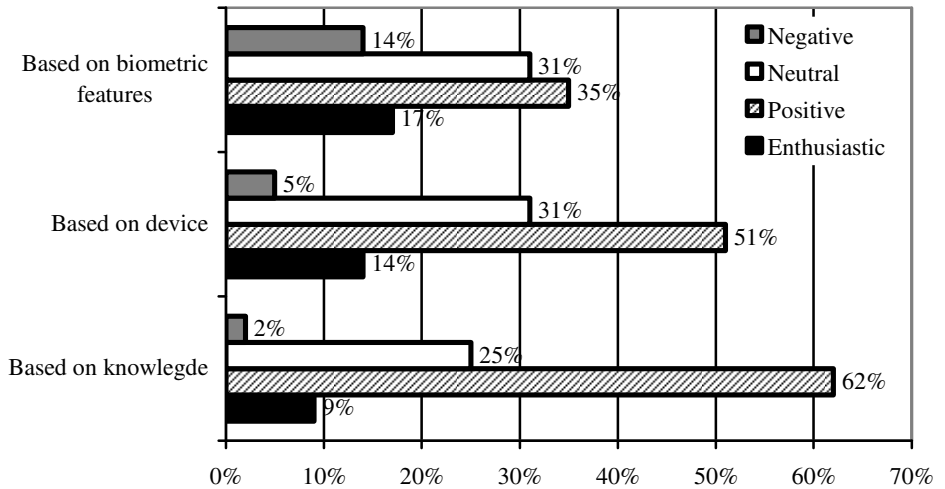

Figure 3. **What is your attitude to the presented method of authentication?,** *own research*

The cause of this result may be the fear of association authentication process with personal sensitive data. About 35% of all the respondents indicate providing enterprise own biometric features or data leak of biometric features as at least one of the two greatest authentication concerns (Figure 4).

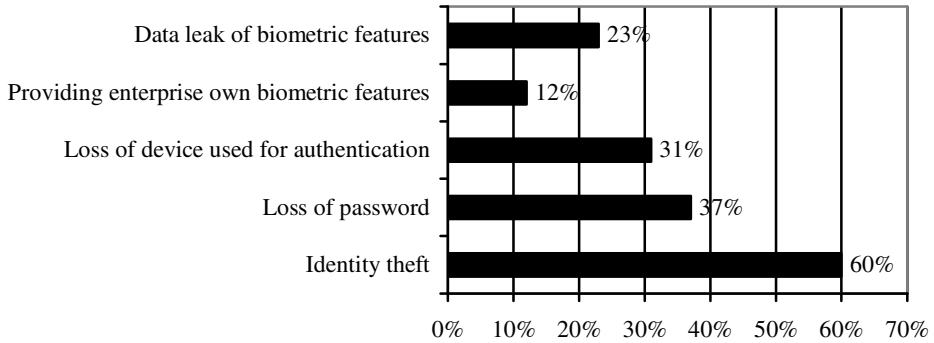

Figure 4. **Indicate maximum two concerns associated with authentication,** *own research*

Identity theft and impersonate user was indicated as the greatest threat associated with authentication (60%). Preventing identity theft is the main aim of more and more sophisticated methods and tools of authentication (Figure 4). The respondents were asked to choose maximum the two threats.

The respondent were asked about the optimal solution for protecting data in information systems. The results are quite interesting.

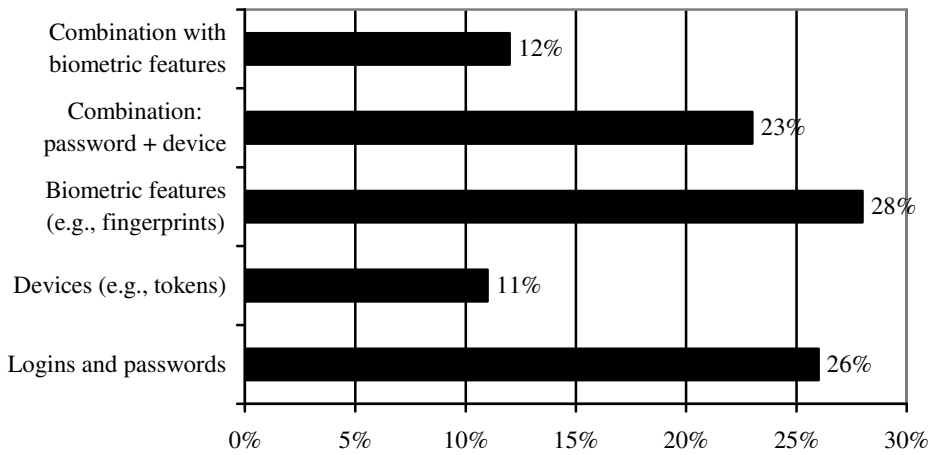

Figure 5. **Indicate the optimal solution for protecting data in information systems,** *own research*

Only 26% of the respondents indicate logins and passwords as an optimal solution for data protection, while using tokens/smart card gained in total 34%, and biometric features in total 40% of the answers. Comparing these results with the answers to the question about the method of authentication used at present, we can conclude that the hypothesis 4 is confirmed.

However, it seems to be incoherent with their attitude to solutions. That is why the reasons of respondents' choice should by carefully studied (Figure 6). Supporters of logins and passwords chose solution comfortable for them (67%) and inexpensive (44%), while others focused on data or method security: 54% in total – device supporters, and 77% in total – biometrics supporters.

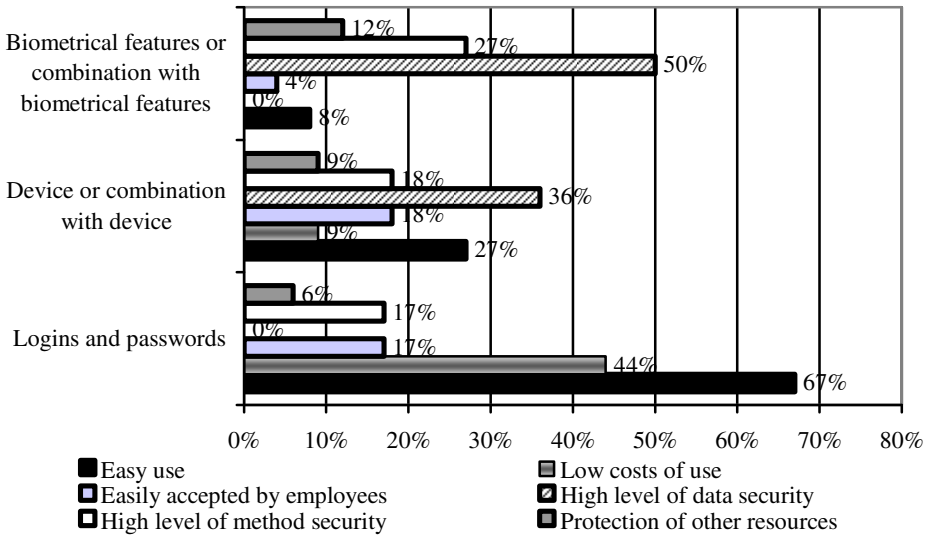

Figure 6. **What are the main benefits of a chosen solution?,** *own research*

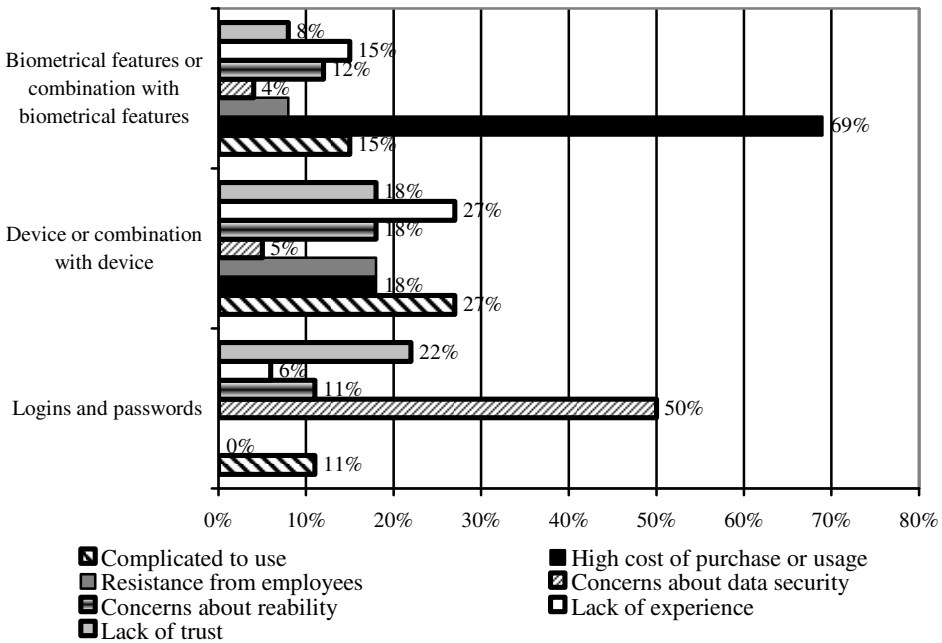

Figure 7. **What are the main disadvantages of a chosen solution which would affect its implementation?,** *own research*

Drawbacks of the indicated method were also studied (Figure 7). For logins and passwords supporters the main obstacle was data security (50%), while for supporters of solutions based on biometrical features – high cost of purchase or usage (69%).

It leads us to a conclusion that there are two groups of users: those for whom the ease of use is the priority, and those, for whom data security is the main concern.

To prove or reject the hypothesis 5, solution chosen by IT professionals and by other employees were compared (Figure 8). The respondents who were not IT professionals selected login and password and biometrical method more often, whereas IT professionals chose mixed, 2-element methods. Thus, we can be formulate the main difference between these two groups: using a single or a combination of methods, thus proving the hypothesis 5.

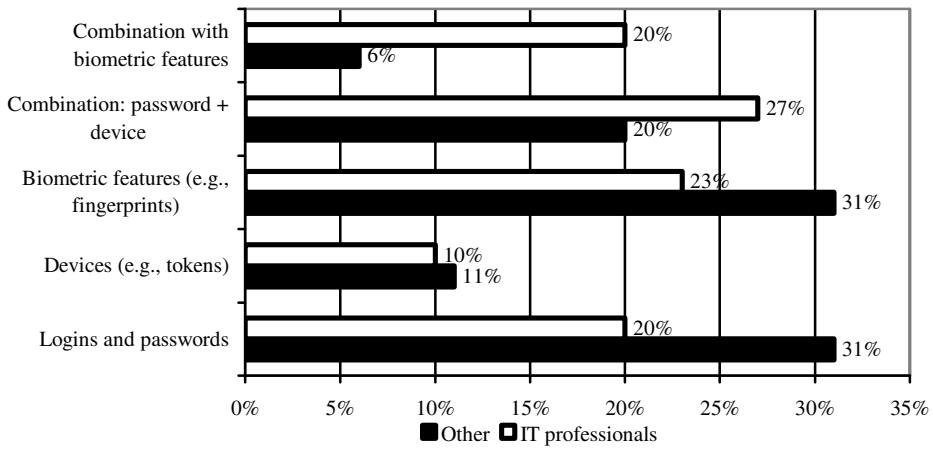

Figure 8. **Result of the task: Indicate one solution which would protect information system resources optimally,** *own research*

Conclusions. SMEs use different methods for authentication, but passwords are still the most common method. Employees are generally opened to new solutions, but while planning implementation, some factors should be taken into consideration:

1. For some employees, especially for non-IT professionals, the ease of use is very important – complicated authentication process may increase employees' resistance and decrease the system security.

2. Although biometrical methods are positively perceived as providing data security, they may affect employee personally, which was one of the respondents' concerns. Moreover, if a company implements authentication based on biometrical features, it must provide high level of reference pattern security.

References:

Ballad, B., Ballad, T., Banks, E. (2010). Access Control, Authentication, and Public Key Infrastructure. Jones & Bartlett Publishers. 398 p.

Burnett, M. (2006). Perfect password. Selection, Protection, Authentication. Syngress. 182 p.

Cross, M., Shinder, D.L. (2008). Scene of cybercrime. Syngress. 732 p.

Felkner, A., Sacha, K. (2010). Deriving RTT Credentials for Role-Based Trust Management. e-Informatica Software Engineering Journal, 4(1): 9–19.

Graham-Rowe, D. (2010). Ageing irises could confound biometric checks. New Scientist magazine, 2771: 2.

Josang, A., Fabre, J., Hay, B., Dalziel, J., Pope, S. (2005). Trust requirements in identity management. In: Proceedings of the 2005 Australasian workshop on Grid computing and e-research (Vol. 44, pp. 99–108). Newcastle, New South Wales, Australia, Australian Computer Society.

Juszczyk, M. (2012). Digital identity acceptance at Polish large enterprises: the survey results. Actual Problems of Economics, 132(6): 496–502.

Kaur, G., Singh, G., Kumar, V. (2014). A Review on Biometric Recognition. International Journal of Bio-Science & Bio-Technology, 6(4): 69–76.

Li, Q.(P.) (2011). Speaker authentication. Springer. 237 p.

Milosz, M., Juszczyk, M. (2012). Individual and Multi-User Digital Identities of Employees in Polish Enterprises – Survey Results. Proceedings of MakeLearn 2012 Management, Knowledge and Learning International Conference, 20–22 June 2012, Celje, pp. 901–908.

Modi, S.K. (2011). Biometrics in Identity Management: Concepts to Applications. Boston, Artech House.

Ran, B. (2013). Global Perspectives on Technological Innovation. Charlotte, N.C., Information Age Pub.

Smedinghoff, Th.J. (2011). Introduction to Online Identity Management. United Nations Commission on International Trade Law, 17.11.2012 // www.uncitral.org.

Windley, Ph. (2005). Digital identity. Sebastopol. O'Reily. 254 p.

Стаття надійшла до редакції 7.11.2014.