UNIWERSYTET TECHNOLOGICZNO-PRZYRODNICZY
IM. JANA I JĘDRZEJA ŚNIADECKICH W BYDGOSZCZY
ZESZYTY NAUKOWE NR 265
TELEKOMUNIKACJA I ELEKTRONIKA 19 (2016) 19-28

SECURITY IMPROVEMENT IN A MOBILE PAYMENT SYSTEM

Mścisław Śrutek[1], Agata Wojciechowska[1], Josep Solé-Pareta[2]

[1]UTP University of Science and Technology,
Faculty of Telecommunications, Computer Science and Electrical Engineering,
al. Prof. S. Kaliskiego 7, 85-796 Bydgoszcz, Poland

[2]Universitat Politècnica de Catalunya (UPC), C. Jordi Girona, 31
08034 Barcelona, Spain

Summary: The mobile payment system and possible ways of using it are presented in this paper. There are a security analysis and a description of a potential risk. A proposal of security improvement is also included in the paper. The proposed solutions may be both safe and comfortable for mobile payment users. This paper is based on the research done as part of the COLIBRI Erasmus+ program and available online documents.

Keywords: mobile payment system, security, COLBRI Erasmus+

1. INTRODUCTION

Modern technologies have been progressively introduced into the people life's. Hardly anybody has thought about children, who readily use tablets, or about the elderly people spending their free time on the Internet. SmartWatch has become a transparent standard combined with the phone function, so has Smart TVs with higher resolution matrices – with access to the Internet, as well as the phones having more computing power than any computer in the past. In light of this progress, revolution in the banking sector is a natural consequence.

Such changes could not occur without participation of scientists from technical universities. In order to study the Future Internet Opportunities, a COLIBRI course has been established as part of the European Erasmus + program [2]. The project includes 7 universities from 7 countries: Denmark (Aalborg University), Norway (University of Stavanger), Latvia (Riga Technical University), Germany (Technical University of Hamburg), Poland (University of Science and Technology in Bydgoszcz), Turkey (Bogazici University in Istanbul) and Spain (Technical University of Catalonia in Barcelona) and three business representatives: Atene mobile in Berlin, Talaia Networks in Barcelona, EKT / NHRF in Athens. The overall objective of the project is work in cross-cultural and cross-disciplinary group upon use of the latest technologies in the field of IT, as well as anticipating future developments and solutions. Some of the ongoing issues relate to economics and entrepreneurship. Moreover, for academic teachers this is an opportunity to get familiar with new learning methods and confront their experiences with the knowledge of lecturers from other countries. The participants of the course are students of the above mentioned universities (3-5 students per university). Together they carry out courses on various topics and participate in workshops (including video lectures, assignments and activities covering the future Internet from different points of view). They are divided into smaller international groups and under the guidance of lecturers they implement various projects according to the latest industrial trends. The themes of the projects cover real problems reported by companies operating on the markets of different countries. One of the projects, implemented in the 2015 course of COLIBRI was '*The personalization vs. privacy tradeoff in a mobile-payment experience*'. The project was carried out on behalf of DINUBE[3], a company from the mobile banking sector in Spain. Dinube was asked for reporting the expectations of the users, and their needs, while the company was interested in getting to know how those expectations should be fulfilled in the best possible way, using the most innovative technology. This knowledge would enable DINUBE to provide more comprehensive services, by increasing mutual trust, thus increasing the number of customers.

Within the scope of this project, online survey was carried out, in order to indicate the opinion of the Internet users on key security issues. As a result, more than 200 respondents from seven countries of Europe provided their answers to the questions of the survey. The survey included, among others, questions about reading the conditions of privacy policy and regular changes of passwords.

The article provides some results of the considered survey and analyses current solutions in the field of mobile payments. Some of the most popular applications and their most important features have been taken into consideration. As a result, an innovative solution has been offered, that can improve the security of mobile payments while maintaining the convenience of use.

The mobile payment market is relatively new and is changing rapidly. For this reason in literature there are only sets of online papers. This set was completed carefully to rely only on very reliable sources, e.g. European Central Bank [4] or the financial branch leader Visa [10]. In this paper there are also references to annual reports. They concern the usage of smartphones, modern technologies and development prospects [7, 8]. In literature there are also links to the Security Research Labs's documents that refer to breaking security measures [5, 9] and link to the COLIBRI course home site [2].

2. MOBILE PAYMENT ANALYSIS

Nowadays each or almost each Pole has a mobile phone. The majority of them (over 60%) uses smartphones [8]. According to the telecommunication companies, the sale of basic phones is constantly decreasing. They try to convince their clients to the smartphones but at the same time they do not withdraw the basic phones from sale. The smartphone possession is closely related to the age and is presented in the Figure 1.

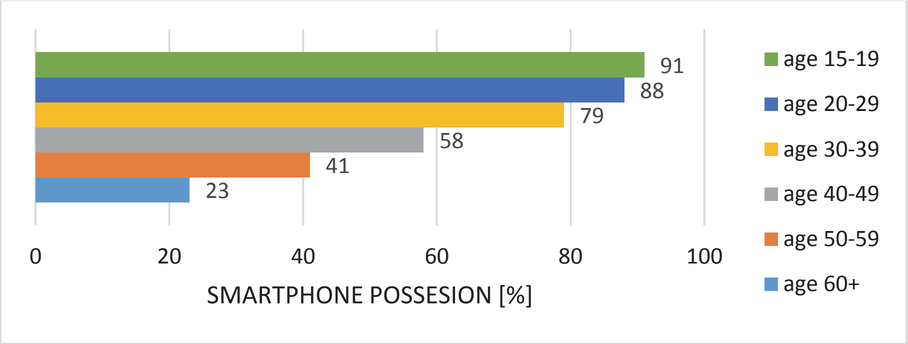

Fig. 1. The smartphone possession in Poland in 2015[8]

Mobile banking is rather a young service. In Poland the first attempt to implement banking operations into the mobile world was in 2000. Because of high prices of data transmission, this service did not belong to the mainstream. Rapid development of the mobile payment system started together with reduction of data transmission prices. Banks and other institutions from the banking sector have been creating and publishing their own mobile applications for about 5 years. These applications are catching users' attention and are constantly changing the clients' attitude to the mobile payment. The figures presented below show how the attitude to the mobile payment has changed since 2013.

Mobile payment has become increasingly popular for the last two years. For this reason most banks provide their clients with a possibility to use a specific mobile application with a wide range of features. There are some features listed in the table below, but the most basic functions including: checking the bank account balance, using bank transfers or paying at a different kind of shops, have been intentionally neglected. They are simple and each mobile payment application can realize them.

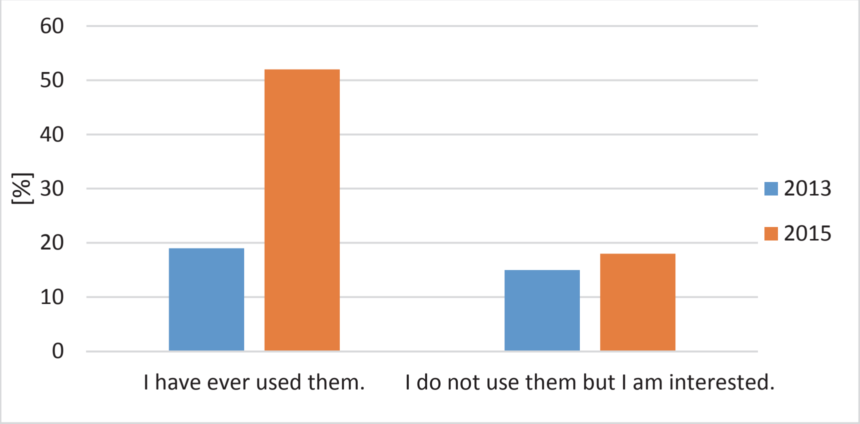

Fig. 2. The changing attitude to mobile payment in Poland from 2013 to 2015 [7, 8]

It is worth seeing that the mobile applications are dedicated to the different kinds of mobile operating systems. Software development focus mainly on the most popular platforms (Android) but still there are some applications for niche operation systems (BlackBerry).

Table 1. Mobile payment applications' functions [6]

Bank	Bank machine	P2P payment	BLIK	Prepaid mobile phone	Operating systems
Bank Pekao	yes	no	no	yes	Android, iOS, Windows Phone, BlackBerry, Symbian
ING Bank Śląski	yes	yes	yes	yes	Android, iOS, Windows Phone, BlackBerry
PKO BP	yes	yes	yes	yes	Android, iOS, Windows Phone, BlackBerry, Symbian
BZ WBK	yes	yes	yes	yes	Android, iOS, Windows Phone
Bank Millenium	yes	yes	yes	yes	Android, iOS, Windows Phone
Alior Bank	yes	yes	yes	yes	Android, iOS, Windows Phone
mBank	yes	yes	yes	yes	Android, iOS, Windows Phone
Eurobank	no	no	no	yes	Android, iOS, Windows Phone
Getin Bank	no	no	no	no	Android, iOS, Windows Phone
Bank BPH	no	no	no	yes	Android, iOS

The column especially worth seeing in the table is the 'BLIK' column. It refers to an additional service that is included in mobile applications form 6 banks (another banking companies will be joining this program over the next months) and is called BLIK [1]. This is the service delivered by Polski Standard Płatności (en. Polish Payment Standard, shortly named as PSP). It has been prepared since 2013, until on 9th of February 2015 it was officially started. In December 2015 there were over 1.5 million of users and over the million transactions done with BLIK. The main features include:

- payment in shops and service points,
- payment online,
- withdrawing cash from banking machine,
- bank transfers using only the telephone number of a recipient.

Moreover there is a special loyalty program for the BLIK users, they may buy cheaper cinema tickets or may have a lower price for VOD movies. Even though the number of the service points that accept this kind of payment is constantly getting bigger, it is still a solution available only on the internal Polish market.

Another way of mobile payment is the HCE (Host Card Emulation) technology using. The most distinctive features of this kind of solution are making use of the NFC (Near Field Communication) module and moving all needed computing into a cloud. Moreover, the owner of a smartphone is not bound to exchange his/her SIM card in order to make the HCE payment possible. The application needed to run the operation is uploaded on the terminal.

When the HCE payment is being performed, a smartphone operates as a common proximity card that may be used to do any contactless operation. HCE operations are available for clients of the Polish banks such as: Getin Bank, BZ WBK or Pekao. However, the requirement for the smartphone to use the HCE payment are Android operating system (version 4.4 KitKat or higher) and NFC module included in the mobile handset. The biggest advantage of this solution is its wide acceptance. By the end of 2017 it will be possible to use the HCE payment in each terminal in Poland while by the end of 2019 in each terminal in Europe. This kind of payment is supported by Visa and MasterCard and thanks to this support it is possible to pay with HCE even in places without access to the mobile network.

However there is still a possibility to use mobile payment with an older type of smartphone (without NFC module) or with an operating system different from Android. This possibility is based on the QR codes. The QR codes are commonly used to keep static information about a bank transfer. They are mostly placed on the invoices coming from mobile operators or electricity suppliers. They include the basic information about the transfer, like a recipient, a topic of the transfer, an amount of money that should be paid. There is another usage of QR codes in mobile payment applications coming from banks. The code is automatically generated in the terminal, users scan this code with their mobile phones and accept the started transaction with their personal PIN numbers.

3. CURRENT SOLUTIONS AND THEIR SECURITY LEVEL

The anonymous online questionnaire was published in order to discover what users' requirements are, and which factors may make the respondents become a mobile payment system users. This survey was done as a part of the COLIBRI program. There were more than 200 answers collected in the questionnaire. However, most of respondents was students of technical universities or engineers. They may concern more about the technological issues. In the former analysis, the survey should be targeted also to other groups of general population.

The figure presented below shows the respondents' answers to the question 'What attributes are strong incentives for you to use mobile payment?'

It comes from the figure that according to the users' answers the most important issue is the privacy (61%). It may be connected somehow with the news published on the Internet and by the press telling about some data leaks. In some cases, sensitive data leaked out from servers of different companies and became public. That may be the reason why respondents are worried about their personal data.

The figure shows also that, according to the users' declarations, they pay a lot of attention to the security (44%). The mobile payment concerns financial issues and losing a big amount of money may cause some serious consequences. Hence, the software companies should pay more attention to the security of the mobile payment. The applications have to be secured from unauthorised access and the security should be absolutely reliable.

However, there is still a relatively big number of users who really do not attach much importance to keeping their private data safe. They appreciate more the possibility of using the mobile payment than security. The great challenge for designers of applications is to take into account both of these requirements.

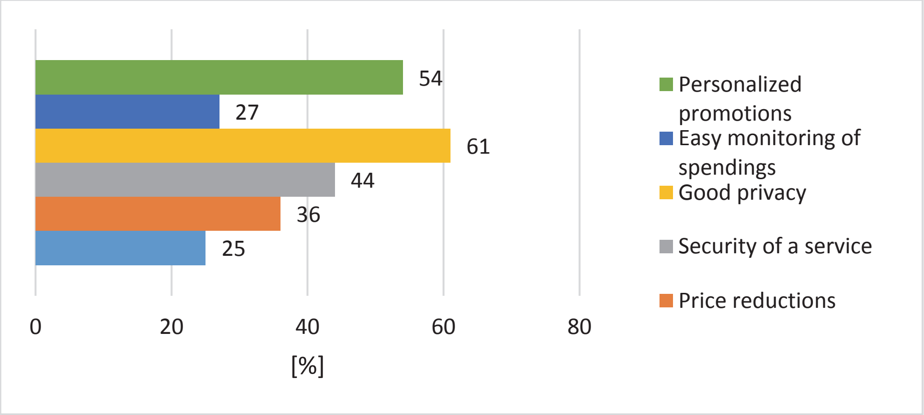

Fig. 3. The online questionnaire's results

In some further paragraphs different ways of security are presented. They refer to the currently used solutions starting from the BLIK [1] system and finishing with data localization. The BLIK system is described as fast, simple and safe. The main authorisation way is a special code. Each code is generated by the PSP as a chain of six random digits. It is valid only for two minutes from the moment of generation. In addition, in order to generate a code, the user has to log in to the mobile payment application which is basically secured with the personal PIN code. The process of a code authorisation in the BLIK system has five steps:

- the code generation,
- putting the code into the terminal,
- the code authorisation by PSP,
- the operation authorisation by the bank,
- transferring an answer to the store.

There are also some possibilities to use biometrical data. Some banking applications may be authorized with the user's fingerprint. This opportunity is given to the clients of banks Millenium, ING and mBank (a service available only for corporation clients). However, in order to enable a biometrical authorisation a user has to possess a selected model of the smartphone, there are for the iOS operating system: iPhone s5, iPhone 6, iPhone 6 Plus and for the Android operating system, there are three Samsung's devices with a special Samsung Pass function available only on the newest mobiles: Galaxy S5, Note 4 and Galaxy S6. Apart from this biometric authorisation it is still possible to log in with a standard PIN code that is composed of four digits.

The security in the HCE payment system is similar to the proximity card security. If the NFC module is active it enables payment right after unlocking the screen and approaching it to the terminal. When the user does the transaction (e.g. shopping) for the amount of money lower than 50 PLN, he/she will not be asked for PIN code. In case of prices higher than 50 PLN, the user will have to enter his/her PIN into the terminal.

There are not many operations that can be performed without any authentication in the mobile payment applications. One of them is checking the bank account balance. It is worth emphasizing that it is the most common operation in mobile banking. It is much faster as the user does not have to enter the password and wait for an authentication. There is a significant difference between the current solution and former ones such as plastic debit card with a small display in the corner (introduced by Getin Bank in 2013). In case of cards, two PIN codes were used in the past. The first one was used only for checking the bank account balance while the second was used for an operation authentication. The majority of mobile applications (like mBank, ING, Millenium) do not show the account's balance directly. At the beginning, the user has to set the maximum balance level and afterwards only the percentage is visible. It may improve the security because nobody knows how big the maximum level is. However, there are still applications (BZ WBK) that without logging in show the account balance in PLN.

Some mobile payment applications use localisation data. After the user's acceptance, the application may analyse his/her position and show the nearest bank agency. In case of the BLIK system, the user may receive the full information about the nearest cash machines, shops and service points that accept payment with a BLIK code.

4. PROPOSAL OF SECURITY IMPROVEMENT

The statement saying that any solution may provide complete safety of the system cannot be true. There is always the element which may break and damage the whole security. Unfortunately, the users seem to be the weakest part of a security system. People are able to remember a countable number of logins, passwords and numeric codes. Furthermore, the knowledge about the potential risk connected with the Internet and the newest technology is decreasing with the user's age.

Some questions about the user's behaviour online was answered in the COLIBRI's questionnaire (Fig. 4, Fig. 5). It was intentional to ask about real habits not about the rule.

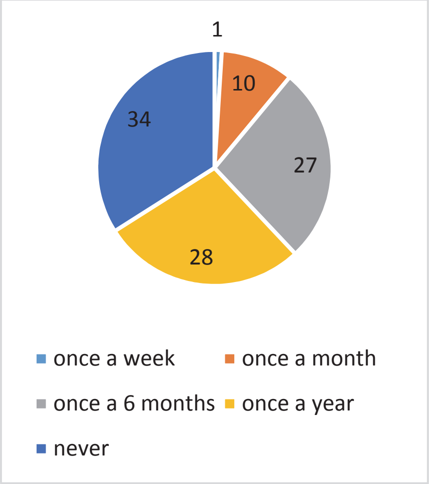

Fig. 4. COLIBRI questionnaire: 'How often do you change your passwords?'

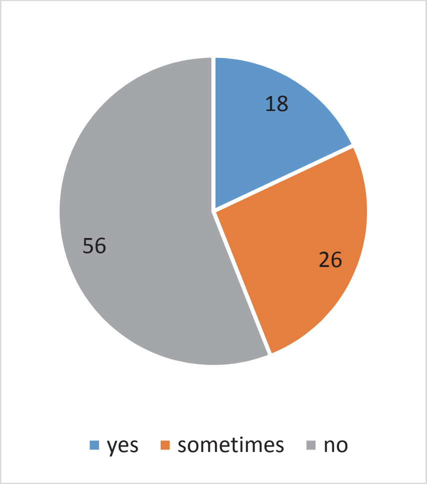

Fig. 5. COLIBRI questionnaire: 'Do you note your passwords anywhere?'

Results coming from two questions were presented in the figures. It is easy to see that one in three users does not change his/her passwords to applications and accounts at all. However, positive is the fact that more than half of respondents do not write down their passwords and codes anywhere.

Unfortunately, current securities sometimes are not good enough to protect the mobile applications from frauds. In further presented paragraphs there are some biggest doubts about each commonly used technology. First of all, there is a PIN code or a password. This is the most basic way of protection of the application. The default code length is four digits which gives about 10.000 potentially solutions. Obviously, the security increases with the password length. Nevertheless, it is possible for a potential thief to check all the possibilities with the current computing power and it would be not very time consuming. Moreover, codes and passwords defined by users are usually relatively short and schematic (e.g. the sequence composed of the same digit or the sequence similar to 12345). People sometimes use bank machines or terminals carelessly. They do not cover the keyboard anyway so that everyone can easily see their PIN code. They do not realize that there may be a small camera installed above the bank machine's keyboard. The next mistake may be writing down the passwords on the small pieces of paper or in case of a mobile payment in the telephone notes.

The HCE payment system is provides security similarly to the proximity card system. Any transaction below 50 PLN is authorised without any confirmation. Hence, in case of stealing of the mobile phone a thief has full access to the user's money. Obviously, transactions may be insured but it depends on the insurance conditions which are described in the agreement in details. There is also a possibility for user to reduce the limit to 0 PLN. In this way the user has to enter the PIN code each time he/she uses the application.

The next way of protection of the mobile payment application is biometrical data. It should be remembered that the fingerprints scanner that are mounted into the mobile devices might be easy to deceive. The Security Research Labs [5, 9], the group of German scientists, proved that this protection can be easily broken. Each person leaves their fingerprints on many places like: a smartphone screen, a computer keyboard, a desktop or even a door. German scientists used the unintentionally left fingerprints, put them on the special foil and prepared the pattern. They were able to unlock the Samsung Galaxy S5 and iPhone 5s by swiping this pattern through the scanner. Moreover, there were some information available on the Internet warning about a possibly wrong storage policy. BMP files with fingerprints are probably stored on HTC and Samsung devices without having proper security.

The last two types of protection are a point unlock (well-known from Android smartphones joining dots in the proper order) and face recognition. Using the point unlock is similar to PIN codes and passwords. This gesture may be seen by an unauthorised person. The second security is not able to detect if there is a real human in front of the camera or maybe there is only his/her photography. According to the above mentioned analysis, the most important threats include:

a) watching by an unauthorised person (a PIN code),
b) counted number of combinations (a pattern unlock),
c) sensitive data storage inside the device's memory (fingerprints),
d) using a fake pattern (a face recognition).

A gesture recognition seems to deprived of these mistakes. The gesture should be natural and possibly done many times during the day, like: smile, eye wink. The software should not compare the user's face with the remembered pattern (no data stored) but only analyse the movement and detect the defined gestures. It may be reasonable to put the gestures in a sequence. In that case only the sequence of proper gestures gives the authorisation to the mobile transaction.

5. CONCLUSIONS

Modern technologies are a great chance for the bank's clients. Payments are getting much faster and more comfortable. Unfortunately, users often forget about the proper security of their data and money. They sometimes prefer more comfortable services than safe services. Most mobile payment systems are presented in this document including their main features and, above all, their potential disadvantages.

Obviously, it should be emphasized that payments done with the mobile phone are not bad or useless. They are really modern, still in progress and comfortable. The application user knows his/her bank account balance and can easily manage his/her expenses. The security of mobile payment applications has to be the priority for banks. Nevertheless, the weakest part of the authorisation chain is the user. The proposed way of protection using a gesture recognition gives the user the maximum of comfort without the risk of losing money.

Now the main aim for banks and other companies from the financial sector should be the education. They should persuade the users that by obeying the rules (not writing down the passwords, changing them regularly etc.), users may help in the mobile payment development. Education and further development of security issues will definitely increase the number of the mobile payment system users.

The research on the mobile banking started at COLIBRI course will be continued. The improvement proposed in this article will be soon implemented and used to create the master project.

BIBLIOGRAPHY

[1] BLIK home web page, access: [01.2016 www.blikmobile.pl].

[2] COLIBRI project web page, access: [01.2016 http://www.tuhh.de/colibri/about.html].

[3] DINUBE web page, access: [01.2016 https://www.dinube.com/en/what-is-dinube/].

[4] European Central Bank 2013. Recommendations for the security of mobile payments.
access: [11.01.2016 https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf].

[5] Goodin D., 2015. Severe weaknesses in Android handsets could leak user fingerprints, access: [09.01.2016 http://arstechnica.com/security/2015/08/severe-weaknesses-in-android-handsets-could-leak-user-fingerprints/].

[6] Klimontowicz M., 2014. Rynek płatności mobilnych w Polsce – stan i perspektywy rozwoju. Annales Universitatis Mariae Curie-Skłodowska vol. XLVIII (3) Lublin.

[7] Mikowska M., 2013. Marketing mobilny w Polsce. Jestem Mobi, Katowice.
[8] Mikowska M., 2015. Polska jest MOBI. Jestem Mobi, Katowice.
[9] Secutiy Research Labs. 2015. access: [09.01.2016 https://srlabs.de/spoofing-fingerprints/].
[10] Visa 2013. Mobile payment acceptance solutions. access: [11.01.2016 https://usa.visa.com/dam/VCOM/download/merchants/bulletin-mobile-best-practices.pdf].

POPRAWA ZABEZPIECZEŃ W SYSTEMIE PŁATNOŚCI MOBILNEJ

Streszczenie

W pracy opisano płatności mobilne i dostępne sposoby ich wykonywania za pomocą smartfonów. Artykuł zawiera analizę bezpieczeństwa płatności mobilnych, a także omawia potencjalne ryzyka kradzieży danych jakie są z nimi związane. Analiza przeprowadzona została na podstawie informacji dostępnych w Internecie oraz przeprowadzonych badań. W dokumencie zawarto również propozycję usprawnienia sposobu zabezpieczeń, która przy zachowaniu wygody mogłaby dobrze służyć użytkownikom płatności mobilnych. Artykuł jest oparty na badaniach przeprowadzonych w ramach projektu COLIBRI Erasmus+ oraz dostępne źródła internetowe.

Słowa kluczowe: system płatności mobilnej, bezpieczeństwo, COLIBRI Erasmus+