Services Of Telecommunication Systems Of New Generation

Valentyn Abakumov, Marina Lyskova

Abstract - **A study of technology of remote payment in mobile communication systems, practical application and data security of these technologies was researched. Comparative description of technology of remote payment of services was conducted in mobile communications: QR-codes, mPos-terminals, applications MasterPass and NFC technologies, taking into account the problem of introduction and principle of work methods of practical application of every technology were offered in the relevant field. On the basis of undertaken studies of methods of providing a safety of data, application AppLocked based on Android was created. The detailed analysis and comparison of the effectiveness of work of technologies with proposed methods of practical application and protection of the systems.**

Keywords - **mobile acquiring, mobile network, algorithm for data transmission, smartphone, MasterPass.**

I. Introduction

A plenty of different solutions are represented at the market of mobile payments, each of that has a right on existence.

The most widespread of them are: mPos-terminals, QR-codes, MasterPass, NFC. Some of them develop successfully enough, other, despite the millions of infusion until now does not justify hopes. In these terms of providing of rational introduction and reliability of techonogies of remote payment of services is very relevant scientific and technical challenge.

One of the possible and perspective ways of solution of the indicated problem is distribution of spheres of introduction of technologies in accordance with their hardware and software, and for reliability of payment systems – increase of strength of communication of data security, due to creation of the AppLocked application.

The purpose of this article is an analysis, comparison and practical application of technologies of the remote payment of services in mobile communication systems and providing of safety of data security.

II. Basic Part

Architecture of decision for realization of service implementation on paying for goods and services for the personal accounts of subscribers is maximally close to architecture of decision in relation to implementation of payments from the bank accounts of subscribers.

This will allow subscribers to use a single application (STK-applet) to perform the same implementation of payments to the TSP both from his or her personal account of operator and banking (card) accounts.

Analysis of safety technologies of remote payment of services in mobile communication systems gave such results, that for safety all payment solutions with the use of mPos-terminal require the permanent physical presence of a plastic card.

Mandatory encryption of data is a special component - card reader, which cannot even decipher the owner of the device.

Client must confirm the money transfer by code that comes via SMS, or electronic signature. Receipt of payment arrives by email or SMS. QR-codes are generated virtually by any standard terminal.

The unique code ensures the safety of personal data of the owner and its resources, as in a result, any confidential information is not required for the transaction. Reading of the virus code that can be depicted over the real one is the threat. Currently only a small number of applications can protect from such threats.

System architecture shown in Fig.1., [1].

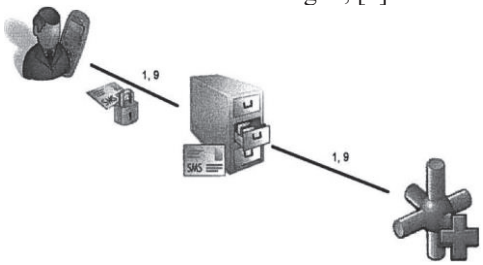

Fig.1. System architecture

Existent methods of remote payment of services and problems of their introduction:

1. MPOS-terminals will significantly increase the number of places where you can pay with an ordinary bank card. With the distribution of mobile scanners paying by card can be anywhere. This mobile solution has the potential to become one of the most productive in the market, and coexist with other remote payment methods.

2. Payments based on technology of reading QR-codes are widely distributed in the first place, because they actually do not require additional hardware costs. But also there is a major defect in that after attachment of the bank card to an application repeated introduction of data is not needed, and in case of stealing of the phone appears a large threat to the bank account.

3. MasterPass has great potential in terms of solving the urgent daily problems of users, and significant advances do not require considerable changes of the

Valentyn Abakumov, Marina Lyskova -. National Technical University of Ukraine "Kyiv Polytechnic Institute", Pobedy Str., № 37, Kyiv, 03056, UKRAINE,E-mail: lmg83@mail.ru.

formed habits. The disadvantage of this technology is the difficulty of implementation, financial and time costs.

4. The development of NFC-payment is rapidly progressing. From one side, rigging of points of receiving payment by NFC-terminals requires significant financial and time costs. On the other hand, NFC supports quite high number of modern models of smartphones, in some countries public transportation, theaters, museums, etc are equipped with this technology. Will NFC widespread or not depends on the number and size of market of participants who will support it.

5. According to recent research hte company «GfK Ukraine» during the second quarter of this year in our country in the final use it was sold 423 thousand of smartphones, but only 11.4% of them, in quantitative terms, with built-in chip NFC. Thus, in view of the market it may be noted that contactless payments in Ukraine through QR-code and mPos-terminal while are looking more promising than using of NFC. Number of smartphones, that can work with NFC and POS-terminals, are able to carry out contactless payments is still very small, POS-terminals, and implementation to MasterPass application requires a lot of time and expense.

As a result of the undertaken study of hardware and software of technologies for remote payment of services in mobile communication systems, it is possible to distinguish the following:

1. The transaction and transfer of the required amount of money with help of mPos terminals requires 2G / 3G smartphone that runs on the operating system iOS or Android mPos-terminal, and most bank cards for payment. It is necessary to establish appropriate solution applications in the smartphone. The principle of mPos-terminals is that the data is read from the credit card reader miniature cards and encrypted via 3G, GPRS or Wi-Fi transferred to the bank processing service, and then to a payment system.

2. At payment with help of QR-codes, in most cases, smartphones or tablets are used as the scanner. For realization of payment it is needed to scan by means of chamber the generated code and to confirm payment in the corresponding program given by a bank. Transfer of data payment to the system comes true by using mobile communication channels or through the Internet. Coding account information in a QR-code scanner can read and pass it through POS-terminal authorization to the bank.

3. For the payment of services and goods through MasterPass you must have a smartphone or tablet, additional equipment is not required. Payments MasterPass for purchases are made within the mobile application which is developed by a company MasterPass. This program will allow to unite all major methods of payment and arrange payments from any point of the world an one touch. The application sends information about the product and its payments through the internet.

4. NFC technology requires an embedded chip in the smart phone or tablet, and contactless payment terminals at retail points of sale. In case of absence of the NFC-module as standard smartphone, it can be set. During the use of NFC it is needed to have a program for its association with bank cards. If you pay via NFC technology transferring of data is over a wireless short-range communication (NFC). In the NFC three basic modes are certain: active, passive and transmission between equal in rights devices.

Taking into account the comfort of using the technologies and compact sizes, it can be assumed that this initiative will become increasingly popular with every year. The main obstacle of implementing of technology remains imperfection of cellular networks. However, every year the situation is improving in this area. Experts predict reduction of the cost of equipment, and therefore more accessible commission and fee rates for mobile acquiring.

Analysis of safety technologies of remote payment of services in mobile communication systems gave such results, that for safety all payment solutions with the use of mPos-terminal require the permanent physical presence of a plastic card. Mandatory encryption of data is a special component - card reader, which cannot even decipher the owner of the device. Client must confirm the money transfer by code that comes via SMS, or electronic signature. Receipt of payment arrives by email or SMS. QR-codes are generated virtually by any standard terminal.

The unique code ensures the safety of personal data of the owner and its resources, as in a result, any confidential information is not required for the transaction. Reading of the virus code that can be depicted over the real one is the threat. Currently only a small number of applications can protect from such threats.

MasterCard and Syniverse are working on a program that will allow to set a limit or even prohibit payment transactions by credit card if location of coupled with it smartphone is different. The program is still being tested, as often, users disable data transfer by coming to another country.

To protect information NFC applies the protected module (SE) - a special storage area in a chip in which access is available only to producers of the chip. In order to read the data, devices must be in close proximity to each other. NFC provides the opportunity of additional introduction of the personal identification number (PIN) for large fees.

The data stored into the device exposed to encryption procedure. For realization of payments permanent numbers of transactions are used.

Thus, each of the payment systems is not perfect in providing security of payments. It requires numerous

improvements and testing to achieve the minimum percentage of breaking the system. Based on data, security development and implementation of application AppLocked, which provides extra data protection, was proposed.

It is possible to identify some positive aspects of existing methods of payment, as a result of the creation of models of practical application of technologies for remote payment of services in mobile communication systems, considering hardware and software:

1. The main positive aspects of mPOS-terminals are compactness and mobility, they are ten times smaller and lighter than usual.

2. The general standard of QR-codes allows users to scan quickly the image, on the obtained pictures via their mobile devices, also to understand what sum and on what account they need to transfer funds using mobile payments.

3. MasterPass provides dealers a convenient way of receiving cash payments regardless of the location of the consumer.

4. The principal advantage of NFC for both consumers and service providers are intuitiveness (it is rather touching for installation of communication), universality (the technology has the widest range of application), openness and compliance with industry standards, capability to support other wireless technologies (initial security through a very small range), interoperability with existing contactless technologies, and the ability to add other security measures.

All the above methods of remote payment are just different ways to approach data. They can coexist as magnetic stripe, chip and NFC-antenna on a plastic card. And sellers, in return, can take the most profitable part of process. For example, in a subway it is better to pay with your smartphone.

In this environment, payments via QR-code, when in the line there are dozens of people, as well as the payment by check-in application will not work. In case of necessity of quick payment NFC is the perfect solution. Each of these technologies will be used depending on the situation and the type of trading. Without doubt they can exist in parallel.

If the owner of the device installs an application, stranger cannot be able to use device, open data with numbers and credit card passwords, check account balance, transfer fees, or use device for payment. The application has an intuitive interface, supports a huge number of features to protect itself.

There are main benefits which enable useful addition of AppLocked and ensure the safe use of technology of remote payment of services in the mobile network:

1. The application is fast enough, almost without loading operative memory and processor unit.

2. AppLocked has an easy and intuitive interface, with which even an inexperienced user can deal.

3. Lock of Android Application is made with using a password or pattern that creates great opportunities for debugging.

4. The application takes only 1.8 MB, while possessing great functionality.

5. There is a fine setting for deferred action, which increases the level of data protection.

6. The function of security settings in certain time allows to block automatically in a preset period.

7. AppLocked can be hided from the phone menu or can be disguised as calculator. It is constructed so in order to protect from stranger.

8. The application can also use a special mode for power saving by minimizing the use of resources.

9. The program is able to backup and restore applications list.

III. Conclusion

The main problem, that interferes the rapid rise of mobile commerce and replacing of simple payment services, is danger in such kind of payments. The second question that must be solved is the vulnerability of information from hackers while using new technologies.

Another problem is the lack of correlation between different financial solutions and platforms. The main obstacle of implementing new technologies is imperfect cellular networks. Each payment systems are not perfect in security payments, and it requires improvements and numerous tests. Basing on security data, development and implementation of AppLocked application was proposed.

AppLocked provides additional protection data in case of loss or theft gadget. When the owner of the device installs an application, stranger cannot be able to use device, open data with numbers and credit card passwords, check account balance, transfer fees, or use device for payment. The application has an intuitive interface, supports a huge number of features to protect itself.

AppLocked partially solves security technology of remote payment of services in mobile communication systems. The judgment may be problems of promotion and popularization of payment services by large companies.

References

[1] Labych «System for mobile bank and electronnic commerce ", Moscow, 2012.

[2] Chris Branden “QR Codes. The Ultimate Guide Book” , *Sreative studios* - 2012 - p.376.

[3] Fisher J. “NFC in cell phones: the new paradigm for an interactive world”, *IEEE Communications Magazine* - 2011 - №6 - p.22.

[4] David Hopkins “QR Codes in Education”, Paperback - October 2013 - p.452.