Analysis of Methods and Practices to Improve the Security of Electronic Means of Payment

Ya. V. Fedorova, A. A. Bykov

Financial University under the Government of the Russian Federation, Moscow, Russia

Abstract. Analysis of the variety of electronic means of payment, which are used in the banking sphere, showed that one of the main banking services now are mobile banking applications. However, security threats in mobile banking have deterred many customers from using it. The issue of elaboration of recommendations, which would allow to strengthen the authentication system to improve security processes, becomes relevant. To achieve this goal, it is necessary to investigate existing methods and practices to improve the security of electronic means of payment. The article presents an analysis of the vulnerabilities of banking applications, technologies for making money transfers, methods for leveling threats in the bank's mobile application system, and fraud protection systems.

Keywords: electronic means of payment, information security, authentication system, mobile banking applications.

DOI 10.14357/20718632230102

Introduction

The modern economy is characterized by a tendency of transition from cash to non-cash means of payment. At the end of 2020, non-cash transactions reached 73% in the structure of financial transactions [1]. In addition, at the end of 2020, the number of transactions in non-cash form exceeded the number of cash withdrawals by 18 times; in monetary terms, the excess was 2.7 times.

At the same time, the demand for Electronic Means of Payment (EMP) among customers is accompanied by problems and risks in these transactions, which causes multiple information security incidents [2]. According to the Bank of Russia's statistics [3], the number of non-consensual transactions in the transfer of funds increased by 40% over a year (in comparison with the 3rd quarter of 2020 and 2021), and their volume in financial terms by 18%. At the same time, the highest dynamics of such operations is observed in the system of remote banking services for individuals.

Analysis of Electronic Payment Means

Analysis of the variety of electronic means of payment used in the banking sphere showed that one of the main banking services now are mobile banking applications. According to the Banki.ru service, the average annual growth rate of mobile application installations is 41.5% [4]. According to the estimates of the Ministry of Finance of Russia and the World Bank in 2020, the share of users of digital banking services has doubled over the past two years - up to 56%. Currently, the users of mobile banking applications are 51% of the population of the country, and Internet banking - 37% (for comparison, similar figures in 2018 were 26% and 16%, respectively) [3].

According to the research, every second mobile application can conduct fraudulent operations and

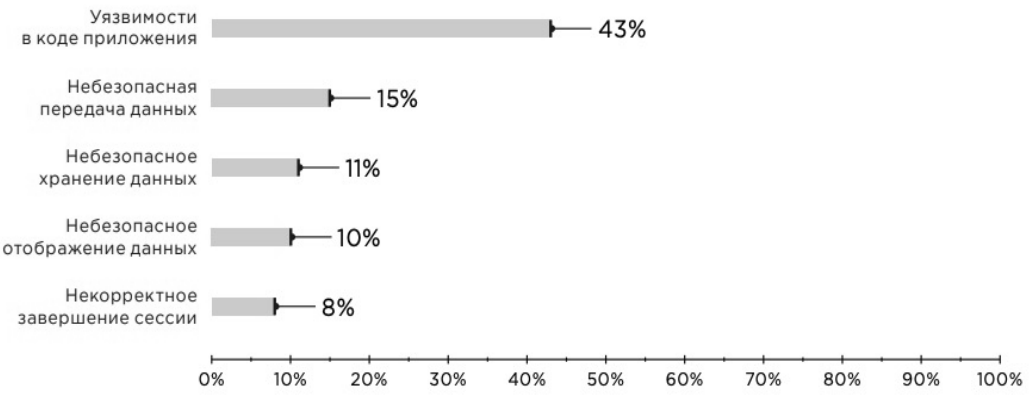

Fig. 1. Statistics of detected types of vulnerabilities in banking applications

steal money: more than 70% of applications have the threat of leakage of customer logins and passwords, more than 30% of applications are associated with incidents of theft of bank card data (Fig. 1) [5].

In addition, the researchers separately assessed the vulnerability of the client part of the application, that is, the mobile application installed on the device, as well as the server part - the web version of the application, which provides remote interaction of the client application with the bank servers through a special interface - API. The results of the study of the client part of the application in the context of mobile operating systems are shown in Table 1 [6, 7].

As can be determined from the data in Table 1, none of the analyzed banking mobile applications is completely secure, regardless of the mobile OS. Even though there is a lower risk of data leakage or information misuse among iOS devices, nevertheless, the average number of vulnerabilities is quite high in both types of mobile systems.

The concept of EMP is defined in the Federal Law of the Russian Federation "On the National Payment System" [8], which was developed in 2011. In accordance with the definition provided in the legislation, electronic means of payment (hereinafter also EMP) is "a means and (or) method that allows the client of the money transfer operator to draw up, certify and transmit orders in order to transfer funds within the framework of the applicable forms of non-cash settlements using information and communication technologies, electronic media, including payment cards, as well as other technical devices".

The last few years have been marked by a significant increase in the use of EMP in Russian practice (Table 2).

As the analysis of Table 2 shows, over 5 incomplete years, the number of completed transactions using ESP increased by 53%, and the volume in monetary terms - by almost 36%. In comparison, the increase in the number of issued bank cards for the specified period amounted to only 19.9%.

A significant problem has been and remains the study of threats to the security of making payments using information technology.

Table 1. Results of mobile banking client application vulnerability analysis according to Positive Technologies

Index	Type of mobile operating system	
	Android	iOS
The level of security of the client part of the application, which has an indicator below the average, % of all applications	92,9	
Distribution of identified vulnerabilities in the client side of the application by OS type, %	53	47
Share of high-risk vulnerabilities, %	3	0
Percentage of medium-severity vulnerabilities, %	40	37
Percentage of low-risk vulnerabilities, %	57	63
Average number of vulnerabilities identified in one mobile application	8,3	7,4

Table 2. Statistics on the use of EMP (mobile applications and Internet banking) by the number and volume of transactions performed in 2017-2021 [author's development]

Period	Number of completed transactions, mln.	Volume of completed transactions, billion rubles	Average volume of 1 operation, thousand rubles
2017	2038,7	1350,50	0,66
2018	2175,2	1675,29	0,77
2019	2789,3	1967,60	0,71
2020	3118,7	1829,35	0,59
1st half of 2021	1557,0	1228,01	0,79
Absolute growth rate of the indicator 2020 to 2017, units	1080	478,85	-0,08
Relative growth rate of the indicator 2020 to 2017, %	153,0	135,5	88,5

To date, the issue of security of the banking system is based on information security technologies that are used by credit institutions. However, this process is also subject to regulation at the state level.

Any money transfer operation, in accordance with federal law [8], must undergo a fraud analysis, for which an anti-fraud (fight against fraud) system is used, that is, a system for responding to fraudulent actions. This provides measures to improve the protection system based on the identified violations. The anti-fraud system detects fraudulent transactions and blocks their execution. Fig. 2 shows a complex for ensuring the protection of information and payments based on EMP [7, 9, 10].

An analysis of the technologies for making money transfers through mobile applications shows that there are two different schemes depending on the number of intermediaries - with one intermediary or several intermediaries.

Analysis of each application showed the presence of 3 vulnerabilities:

1) Lack of protection against code injection and repackaging. That is, in fact, none of the banking applications considered are protected against the introduction of untrusted data or an attempt to bypass verification when receiving information from the web server.

2) No code obfuscation. An obfuscator program eliminates attempts to introduce file changes inside the program (patches), which allow cheaters to gain access to more information, including the source code. That is, the first two problems are interrelated. In fact, the obfuscation method should complicate the existing code, hiding the logic of its operation. At the same time, this method is currently absent in working mobile applications;

3) Using class and method names in code. This simplifies access for attackers to obtain code information due to its simplicity.

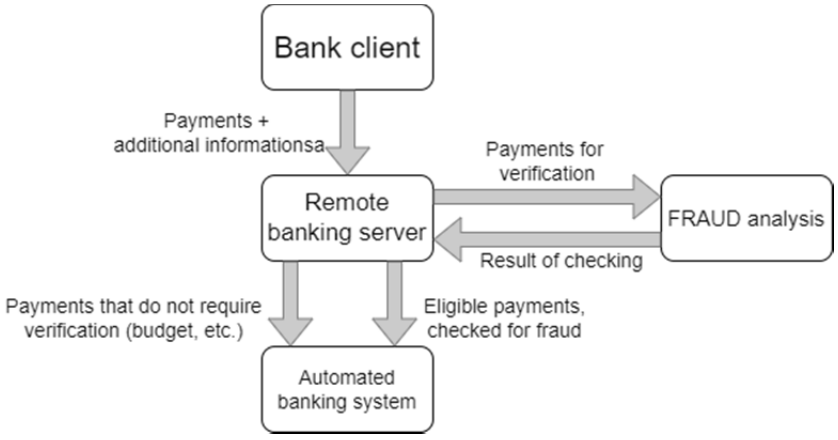

Fig. 2. Technologies for verifying translations based on EMP

Risks when Using Banking Applications

Thus, modern mobile applications of banks have a large number of risks of unauthorized use of information. At the same time, these vulnerabilities were identified both in the client part of the application (that is, in the mobile application directly installed on the client's mobile device) and in the server part of the application, when transferring data from the mobile application to the bank's information system (Fig. 3) [7].

Traditionally, banking organizations have used a defense in depth model. This model has several levels of security control. Thus, if avulnerability exists at one of the levels, then other systems will be protected by other means of protection, and the impact of the compromise will be limited. These levels of security also increase the time it may take for an attacker to break into a bank's system, giving the internal security system more ability to stop an attack.

Today, as applications move to the cloud or use third-party services, banking organizations are increasing their vulnerability and expanding their attack zone. Critical apps share sensitive information with the bank's mobile apps. This leads to interconnected risk. In an interconnected environment, a single misconfigured system or security vulnerability can compromise all information on a mobile device.

Many of today's defense-in-depth strategies are rendered irrelevant by the interconnectedness of data. Ransomware, like other malware, misconfigurations or stolen credentials can be used to break any layer of security before the application layer.

Mobile banking applications support the main functions and processes between the bank and the client. Attackers who have gained access to the mobile application can steal the funds of a bank client through fraud using EMP, which falls under Article 159.3 of the Criminal Code of the Russian Federation.

Traditional vulnerability management solutions do not fully align with bank applications. Without proper threat engineering at the start of mobile app development, and rapidly changing opportunities for data breaches, organizations face a growing backlog of vulnerability patches and often lack the prioritization tools they need to manage updates due to the high frequency of releases and the complexity of vulnerability remediation processes.

Securing a mobile device is possible with an understanding of how intruders gain access to that device.

Analysis of banking practices shows the spread of the following methods of leveling threats in the system of mobile applications of the bank:

1) Enabling multi-factor authentication. The requirement to enter a single password before granting access to a customer's bank account is an insufficiently reliable protection system.

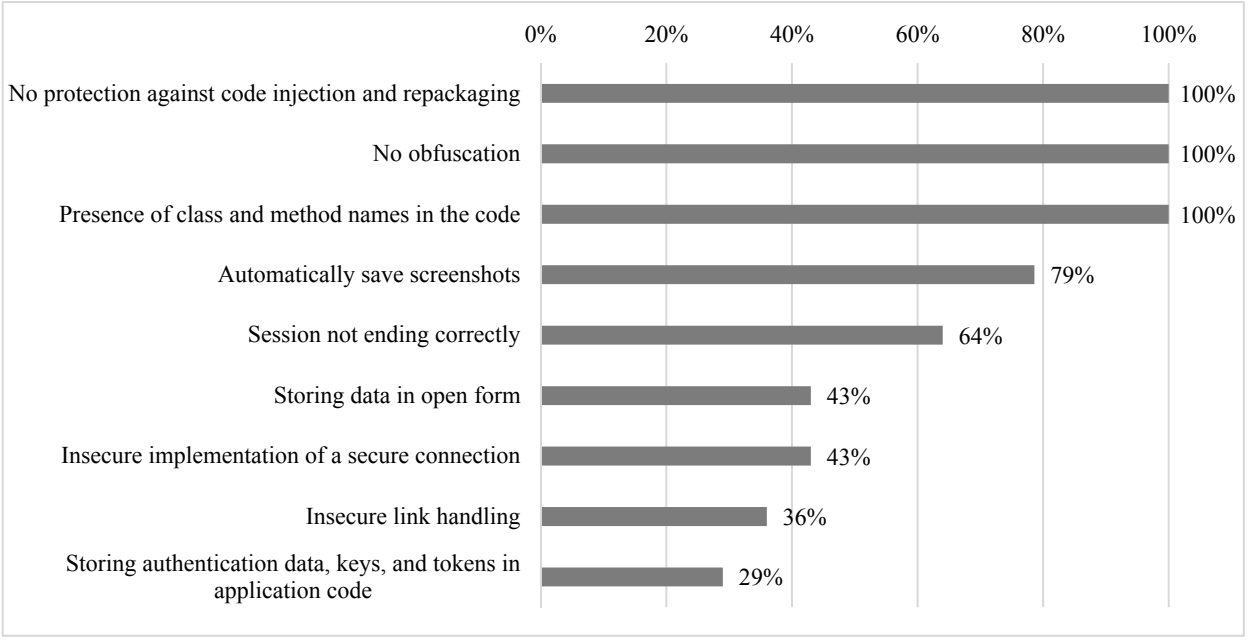

Fig. 3. Frequency of vulnerability detection in mobile apps by type, % detection among surveyed apps

2) End-to-end encryption of mobile banking applications that ensures the safety of data.

3) Use of fingerprint technology (such as iOS-based TouchID). The introduction of fingerprint devices adds an extra layer of security to mobile banking applications.

4) Analysis of customer behavior. With this technology, a mobile banking application can flag business logic errors, abnormal behavior, or unauthorized access for further investigation.

5) Using secure access to the Internet.

The above methods will provide strong authentication for mobile banking solutions and banking service providers. However, it is important that customers also take their own precautions when enhancing the security of mobile banking apps.

Methodologies for Ensuring Information Security in Mobile Banking

In current practice, there are many current standards, methods, methodologies and other approaches to secure software development, which are shown in Fig. 4.

Let's consider the existing methodologies from the point of view of their application to the mobile applications of banks.

In particular, let's take a closer look at the SDL - Security Development Lifecycle methodology developed by Microsoft. This methodology is represented by a set of practices that are aimed at improving the security of the developed software. The SDL methodology is presented as a specialized process that contributes to the achievement of an appropriate level of security for the developed software. SDL is a software development process that provides an assessment of the level of security prior to the final release of the software.

The benefit of Microsoft SDL is to reduce the actual cost of software security development through early detection and remediation of existing vulnerabilities.

Thus, Microsoft SDL operates on the principle of a risk-based approach, since it is not aimed at eliminating vulnerabilities after the fact, but at their preliminary reduction to an acceptable level.

There are a number of models, systems, configurations, processes and preventive measures that are used to prevent credit card fraud. This reduces the financial risks for the bank customer. Specific methods such as the Markov model, application of artificial intelligence, sequence alignment, data mining methods, multiple cryptographic algorithms and genetic programming methods are of

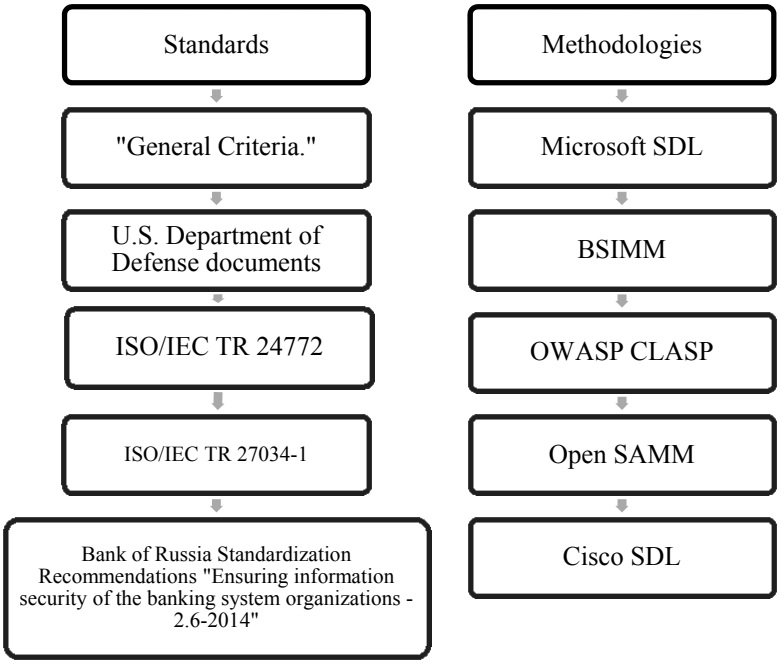

Fig. 4. Basic standards and methodologies in the field of information security in the development of software on which the development of mobile banking applications will be based

Table 3. Overview of antifraud systems

System name	Technologies used
Antifraud payler	Filter "If-then", scoring
Fraud-analisys, BSS Group	Filter "If-then"
SmartVista Fraud Prevention, BPC Banking Technologies	Filter "If-then"
Kaspersky Fraud Prevention	User environment analysis
Fraudwall, Frodex	Filter "If-then", blacklist outsourcing
Answerpro	Filter "If-then"

particular relevance in combating this type of fraudulent transactions.

Anti-fraud systems have recently become widespread. These systems are based on methods of data analysis using artificial intelligence models. At the moment there is a need to modify existing algorithms, develop a synthesis of their application in order to obtain a reliable result. That is why the introduction of big data processing technologies, the so-called Big Data, is becoming urgent for banking systems. A comparative analysis of known fraud protection systems is presented in Table 3.

Analysis of the data in the table shows that most Russian fraud protection systems are implemented using a set of "If-then" rules.

Conclusion

Foreign systems are more functional than Russian systems - the analysis of fraudulent payments is carried out mainly by methods of machine learning. However, foreign systems, as a rule, are not available to Russian banks, and their application is limited by the specifics of Russian legislation. Foreign companies combine different methods to find fraudulent transactions, which makes them more reliable and attractive to customers. The most promising solution today is the use of Unusual Event (UE) detection technologies in combination with machine learning techniques. The use of machine learning is a necessary metric because a large amount of UE information is collected and applying rules to this data becomes impossible.

Analyzing the Russian experience, it is worth noting the lack of legal regulation of antifraud systems. In this regard, mobile operators and banks have been independently trying to create a system that would counter fraudulent activities through electronic banking and ensure the safety of funds in the bank customers' accounts. Several major Russian banks and mobile network operators tested the so-called anti-fraud platform in the first quarter of 2020. Based on the results of the testing, Tinkoff Bank and mobile operators Tele2, Megafon, MTS and Tinkoff Mobile launched the Tinkoff Call Defender platform.

References

1. Gorodnova N.V. 2021. Analiz riskov i bezopasnosti sistemy elektronnykh sredstv platezha [Analysis of risks and security of the system of electronic means of payment]. Ekonomicheskaya bezopasnost′ [Economic security] V.4, №2:401-420.
2. Trautman, Lawrence. 2013. E-Commerce and Electronic Payment System Risks: Lessons from Paypal. SSRN Electronic Journal. 10.2139/ssrn.2314119.
3. Review of reporting on information security incidents in the transfer of funds. 1st quarter 2021. Bank of Russia. Available at: https://cbr.ru/analytics/ib/review_1q_2021 (accessed June 30, 2022).
4. Study of mobile banking applications in Russia. Available at: https://ict.moscow/research/issledovanie-prilozhenii-mobilnogo-bankinga-v-rossii (accessed June 30, 2022).
5. Aleksandrov A.G. and etc. 2018. Analiz ugroz bezopasnosti informatsii pri upravlenii denezhnymi sredstvami s ispol′zovaniyem mobil′nykh ustroystv [Analysis of information security threats when managing money using mobile devices]. Modelirovaniye, optimizatsiya i informatsionnyye tekhnologii [Modeling, optimization and information technology] V6. №3: 234-242.
6. Bolotnova E.A., Pozoyan D.P., Gomolko N.V. 2020. Analiz razvitiya elektronnykh sredstv platezha [Analysis of the development of electronic means of payment]. Vestnik Akademii znaniy [Bulletin of the Academy of Knowledge] №3(38):319-324.
7. Mansi Bosamia. December 2017. Mobile Wallet Payments Recent Potential Threats and Vulnerabilities with its possible security Measures. Conference: 2017 International Conference on Soft Computing and its Engineering Applications (icSoftComp-2017). At: CHARUSAT, Changa, India.
8. Federal Law of June 27, 2011 No. 161-FZ “On the National Payment System” of June 27, 2011
9. Polozheniye Banka Rossii ot 29.06.2021 №762-P «O pravilakh osushchestvleniya perevoda denezhnykh sredstv» [Bank of Russia Regulation No. 762-P dated June 29, 2021 “On the Rules for Transferring Funds”]. Vestnik

Banka Rossii [Bulletin of the Bank of Russia]. №62. – 08.09.2021.
10. Postanovleniye Pravitel′stva RF ot 01.11.2012 №1119 «Ob utverzhdenii trebovaniya k zashchite personal′nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal′nykh dannykh» [Decree of the Government of the Russian Federation of November 1, 2012 No. 1119 “On approval of the requirement for the protection of personal data during their processing in personal data information systems”]. Sobraniye zakonodatel′stva RF [Collection of legislation of the Russian Federation]/ 05.12.2012. №45. article.6257.

Fedorova Yana Vladimirovna Department of Information Security of the Financial University under the Government of the Russian Federation, Moscow. Associate Professor, Candidate of Economic Sciences. Number of publications: 60. Research interests: information security, machine learning. E-mail: fyv21@mail.ru

Bykov Artem Alexandrovich. Department of Data Analysis and Machine Learning, Financial University under the Government of the Russian Federation, Moscow. Associate Professor, Candidate of Technical Sciences. Number of publications: 69 (including 2 monographs). Research interests: data analysis, geotechnical control, digital signal processing, software design. E-mail: arabykov@fa.ru