POSITIVE TECHNOLOGIES

FINANCIAL APPLICATION VULNERABILITIES

2018

CONTENTS

INTRODUCTION

Banks have long been a favored target of digital attackers. Fortunately, financial institutions are well aware of this fact and are loathe to lose clients and money due to cyberattacks. To minimize the risks, banks rely on in-house or outside specialists to analyze the security of their e-banking systems. Such analysis helps to detect vulnerabilities in online and mobile banking applications and provides the information necessary to eliminate vulnerabilities.

Every year, Positive Technologies assesses the overall security level of e-banking applications based on the systems it has tested for clients in the banking industry. This report contains statistics and results from analysis of online and mobile banking applications tested by Positive Technologies in 2017. The findings indicated here do not necessarily reflect the current state of other companies in the same sector. Rather, this information is intended to promote a better understanding among information security specialists of the most relevant issues in a particular sector, as well as assist in timely detection and remediation of vulnerabilities.

EXECUTIVE SUMMARY

The security level of financial applications is improving. The percentage of e-banking systems with critical vulnerabilities has tended to fall in recent years. Critical vulnerabilities were detected in 90 percent of systems in 2015, 71 percent in 2016, and only 56 percent in 2017. Banks are prioritizing critical vulnerabilities in their security efforts.

This year, financial applications based on ready-made vendor solutions contained fewer critical vulnerabilities than in-house applications. Vendors have started to pay more attention to security issues, while banks still lack experienced developers and a mature Secure Software Development Lifecycle (SSDLC).

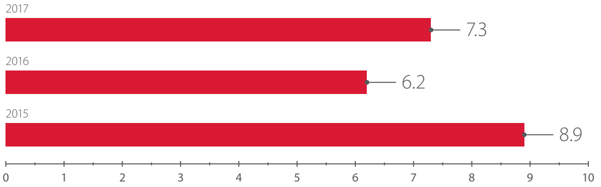
In 2017, the majority of analyzed systems (61%) were in production and accessible to clients. As in previous years, production applications contained a higher average number of flaws than testbed systems still in development. However, the difference was insignificant: 1.7 critical vulnerabilities per production system versus 1.6 critical vulnerabilities per testbed system.

One third of online banks did not have any critical vulnerabilities, while in 2016 high-risk vulnerabilities were detected in almost all financial applications (with one exception). Based on the vulnerabilities found, the main threat for online banks is access to sensitive client information and personal data. The vulnerabilities found at 94 percent of online banks could have been used by attackers to obtain such data.

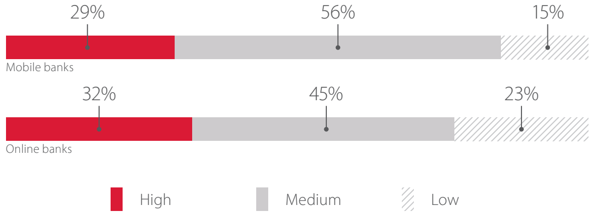
Security of a mere 8 percent of mobile banking applications was graded as "acceptable" (defined as the absence of critical vulnerabilities). iOS applications were better protected than their Android counterparts. Critical vulnerabilities made up 25 percent of the total number of vulnerabilities found in iOS applications; for Android, the equivalent figure was 56 percent.

In 2017, compared to the previous year, the security level of financial applications improved due to the generally lower severity of vulnerabilities

Vulnerabilities per system rising slightly while the severity of vulnerabilities declines

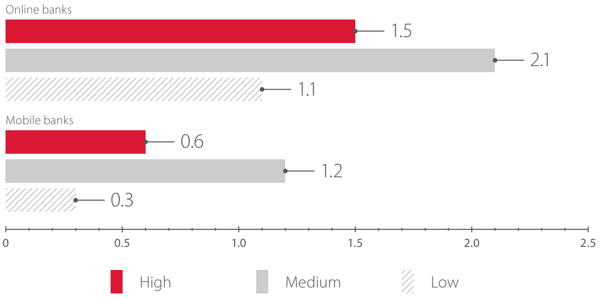


Average number of vulnerabilities per application



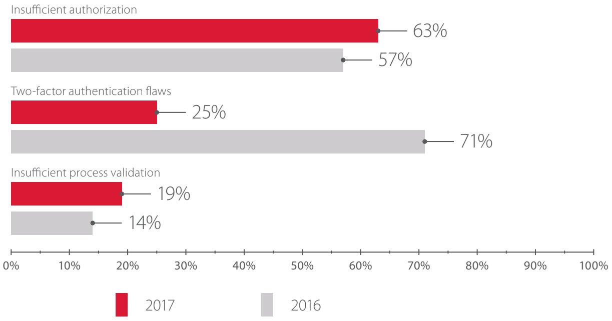
Vulnerabilities of different severity levels

Online banking applications tend to contain more vulnerabilities than mobile banking apps

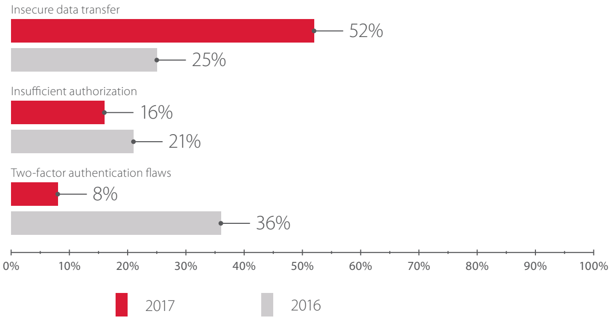


Average number of different severity vulnerabilities per application

Most vulnerabilities involve identification, authentication, and authorization



Critical vulnerabilities in online banks



Critical vulnerabilities in mobile banks

1. RESEARCH DATA

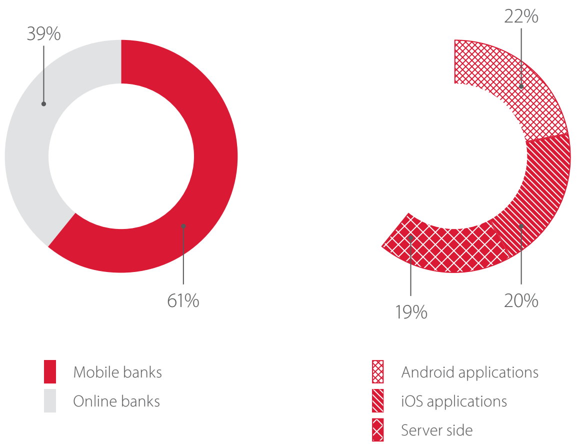
Data comes from audits performed by Positive Technologies during 2017. This report encompasses work performed on 41 applications used for financial transactions.

Most of the tested systems (61%) are mobile applications, consisting roughly equally of mobile app server and client sides for Android and iOS.

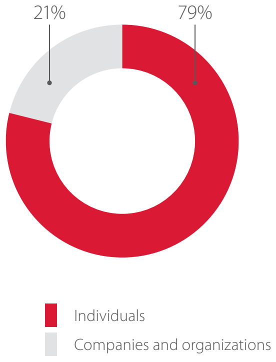
Most of the tested systems were intended for individuals (79%), with the remainder for corporate clients (21%).

The percentage of in-house applications decreased from 78 percent in 2016 to 68 percent in 2017. However, such applications are still used more often than off-the-shelf systems based on platforms from known vendors. In keeping with responsible disclosure of vulnerabilities, no vendors are named in this report. Banks continue to prefer Java (in 46% of cases) when developing e-banking applications.

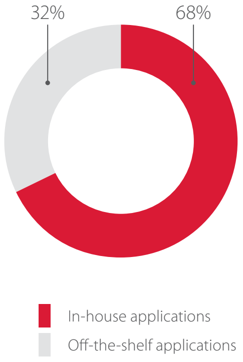
Most analyzed systems were operating and available for clients (61%). The remainder (39%) were testbed applications ready to go into production.



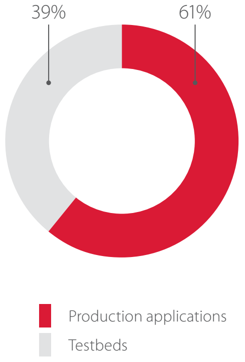
e-Banking system types



Client audience for
e-banking systems



Shares of in-house vs.
off-the-shelf applications



Ratio of production
to testbed applications

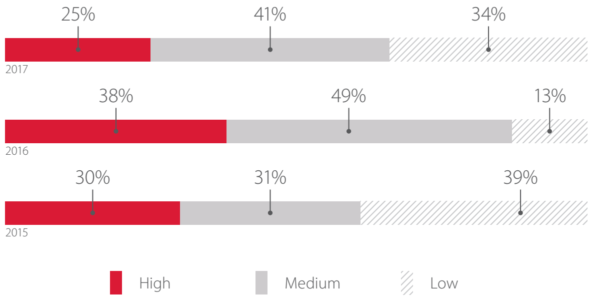
2. PROTECTION FLAWS

2.1. Overall statistics

Every application had multiple security flaws

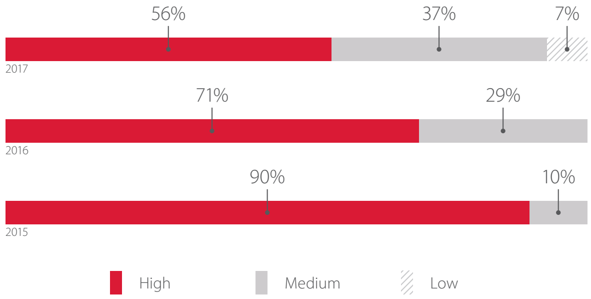
In 2017, an e-banking application contained an average of seven vulnerabilities, which is greater than the previous year's figure of six flaws. The distribution of vulnerability severity changed greatly. High-risk vulnerabilities and medium-risk vulnerabilities both made up a smaller portion of the total (by 7% and 8%, respectively). High-risk vulnerabilities were detected in "only" 56 percent of tested systems. Every year this figure goes down. In 2015, high-risk vulnerabilities were found on 90 percent of systems. Then in 2016, this figure fell to 71 percent of systems. These results suggest that companies are honing in on critical vulnerabilities.

In 2017, the percentage of high- and medium-risk vulnerabilities decreased

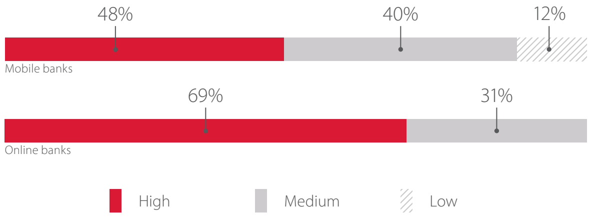


Vulnerabilities by different severity levels

The security level of financial applications is growing, slowly but surely

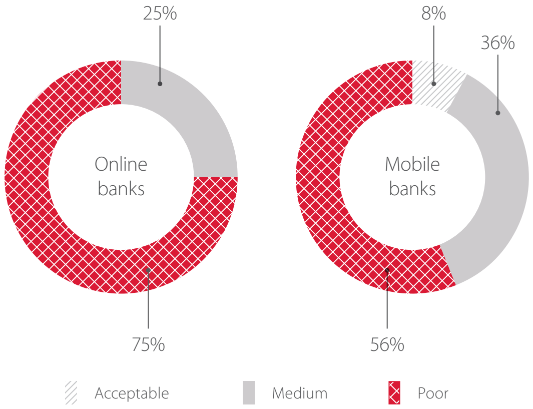


Most severe vulnerability found (percentage of applications tested)



Most severe vulnerability found (percentage of online and mobile banking applications)

Mobile applications are becoming more secure. In 8% of cases, system security was "acceptable." In 2016, 93% of mobile banking applications had a "poor" security level



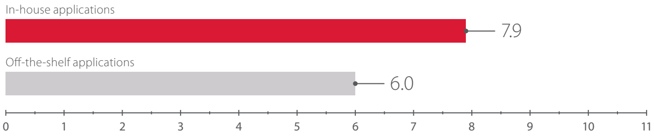
State of security (percentage of applications tested)

Most of the tested applications (68%) were developed by financial companies in-house

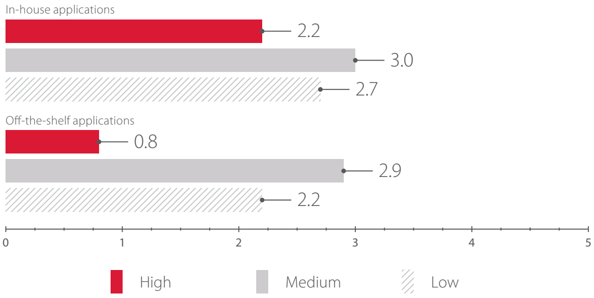
2.2. Comparison of in-house and off-the-shelf applications

In previous years, our statistics showed that in-house banking applications were more secure. In 2016, in-house applications contained only half the number of vulnerabilities in off-the-shelf solutions. But in 2017, the situation changed: the number of vulnerabilities in off-the-shelf solutions decreased significantly. The number of flaws in in-house banking systems increased. Moreover, off-the-shelf applications also contained fewer critical vulnerabilities. Most flaws in in-house applications are caused by code vulnerabilities. This means that banks should pay more attention to training their programmers in best security practices and implementing SSDLC methodologies.

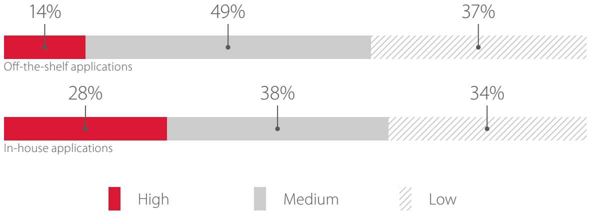
Vendors often do not customize systems to suit the needs of individual banks, leading to flaws in protection mechanisms such as authentication and authorization. In such case, the fault lies not with programmers, but with the management in charge of designing and specifying requirements for the system.



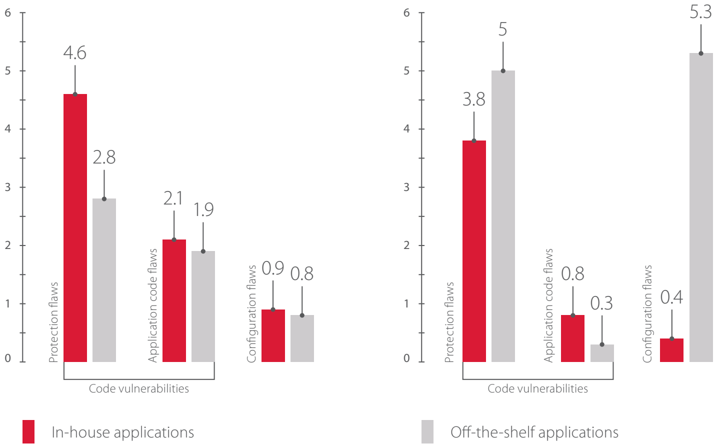
Average number of vulnerabilities per application



Average number of vulnerabilities of different severities in a single application



Vulnerabilities by severity level



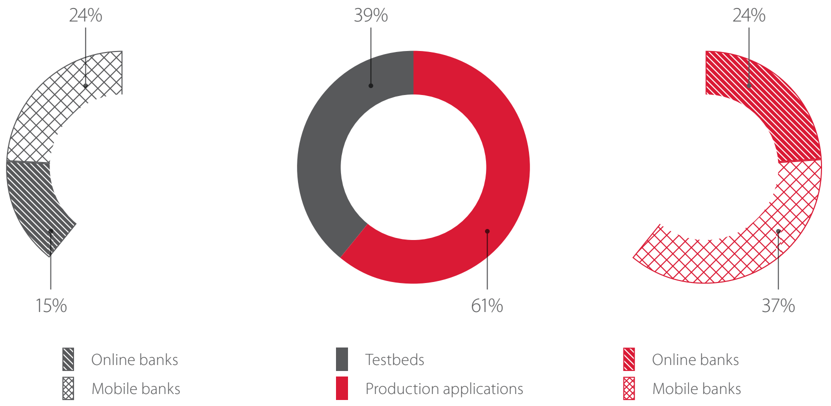
Average number of vulnerabilities per application (2017)

Average number of vulnerabilities per application (2016)

2.3. Comparison of testbed and production applications

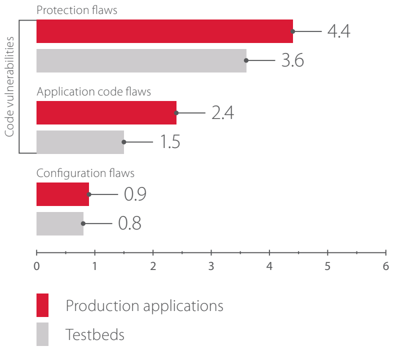
In 2017, most of the tested applications (61%) were in production and available to clients. Security analysis of an application before putting it into production allows taking measures for improving the application and foreseeing all possible security threats in good time, without the risk that an attacker will be the first to find and exploit them. This is the advantage of analyzing an application before making it available to clients. However, regular monitoring of production applications is just as important. New functionality and tweaks may bring new vulnerabilities.

Production applications had **twice as many vulnerabilities** as testbed systems

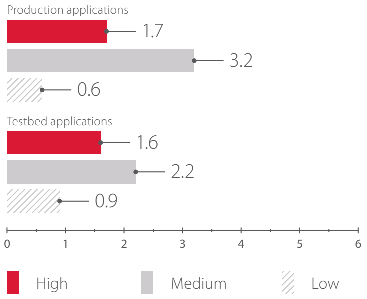


Testbed vs. production applications

As in previous years, the average number of vulnerabilities in production applications was higher than in testbed systems. Most security issues, in both testbed and production applications, were caused by vulnerabilities in code. A common way to minimize such vulnerabilities is to practice a Secure Software Development Lifecycle. For timely identification of vulnerabilities in code, it is necessary to perform regular audits of code quality, such as with white-box testing (including with use of automated analysis tools).



Average number of vulnerabilities of various categories in testbed and production applications

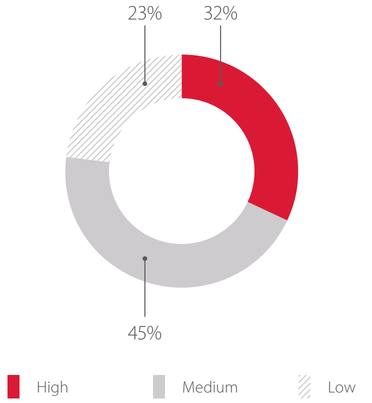


Average number of vulnerabilities of various severity in testbed and production applications

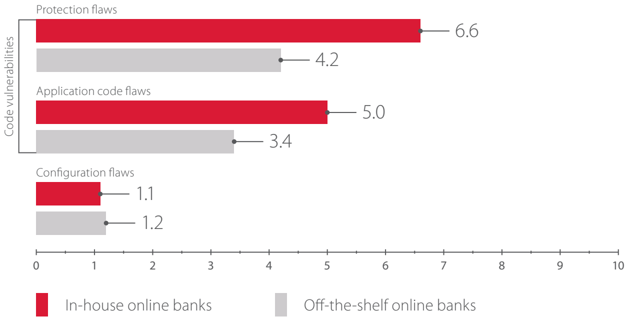
3. VULNERABILITIES AND THREATS IN ONLINE BANKING SYSTEMS

In 2017, we saw an increase in the security level of e-banking systems, in both online banking and mobile applications

No critical vulnerabilities were detected in 31 percent of online applications. By contrast, in 2016, all tested applications (except for one) contained critical vulnerabilities. Each web application had 1.3 high-severity vulnerabilities on average, which is a better result than 2016 and its 2.1 per application (compared to 4.2 per application in 2015). Part of this improvement is due to the fact that some banks already had their systems tested and remediated vulnerabilities in previous years, before turning to Positive Technologies again in 2017.

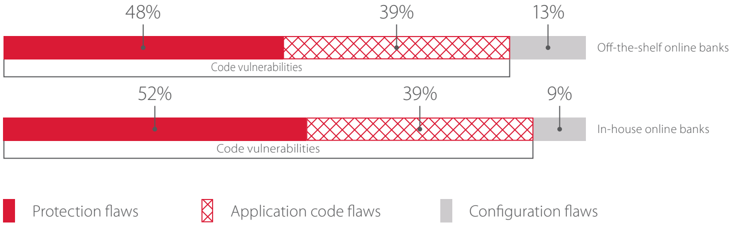


Online banking vulnerabilities by severity level



Average number of vulnerabilities of various categories (online applications)

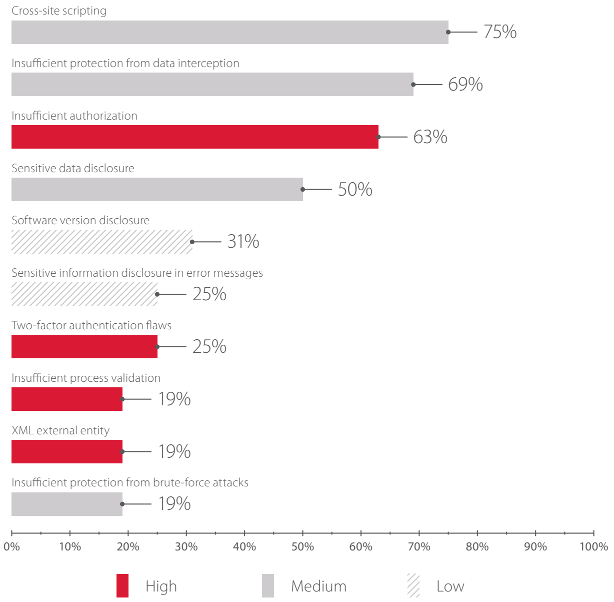
In 2017, the distribution of vulnerability types was similar across in-house and off-the-shelf applications. In-house web applications contained 4 percent more security flaws in implementation of security mechanisms (insufficient authorization or authentication, weak password policy), while applications based on off-the-shelf solutions had 4 percent more configuration vulnerabilities (insecure configuration of HTTP server headings).



Vulnerabilities by category

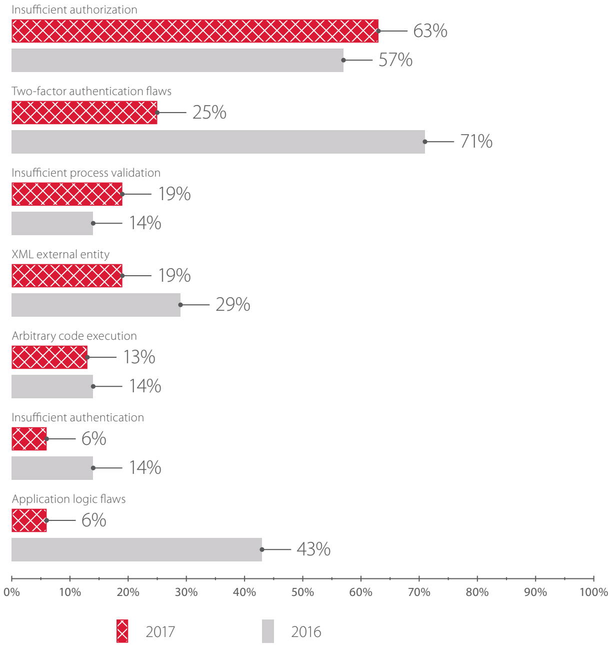
100% of online banks had flaws related to implementation of protection mechanisms

The list of most common vulnerabilities is similar to last year's. The most common vulnerabilities in 2017 were Cross-Site Scripting and Insufficient Protection from Data Interception, which allow attacking bank clients (for example, by intercepting cookies and stealing credentials). More than half of online banking apps (63%) featured insufficient authorization: by exploiting this high-severity vulnerability, an intruder can access web application functions not intended for the intruder's user level.



Top 10 online banking vulnerabilities

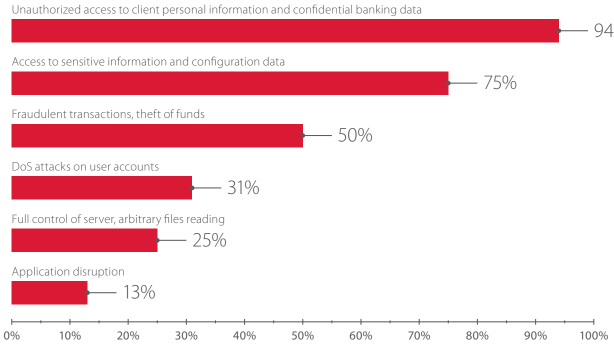
In 2017, critical vulnerabilities of almost all types became fewer in all financial applications. Most high-severity vulnerabilities (63%) involved improper implementation of authorization. Using this kind of vulnerability, an attacker could target bank clients and obtain unauthorized access to sensitive banking information. For example, one of the analyzed online banking applications allowed an intruder to access the web server control panel and change system settings. In another application, an attacker had the ability to learn the balance of other users.



Critical vulnerabilities of online banks

There was also a significant decrease in the percentage of two-factor authentication flaws. In 2017, these vulnerabilities occurred in a quarter of online banking applications (as compared to 71% in 2016). Most of the vulnerable applications lacked protection against one-time password bruteforcing (password lifetime and/or entry attempts were not limited). It is worth noting that cybercriminals can "subscribe" on the darknet to receive the text messages sent to any phone number, enabling them to obtain one-time passwords. That is why banks should take additional measures to secure user transactions.

Vulnerabilities in financial web applications create large reputational and financial risks for banks and their clients. Security gaps can cause very tangible impacts: half of applications were vulnerable to fraudulent transactions and theft of funds. In 94 percent of analyzed applications, an intruder could access clients' personal information and sometimes even sensitive banking data (such as credit card information, account balance, and loan repayment schedules). In one third of web applications (31%), servicing of particular accounts could be disrupted, and 13 percent of applications could be fully disrupted.



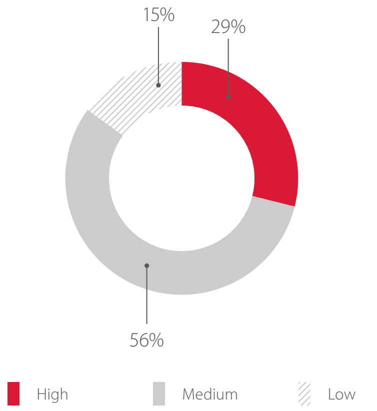
Potential impact of attacks on online banks (vulnerable applications)

4. VULNERABILITIES AND THREATS IN MOBILE BANKING APPLICATIONS

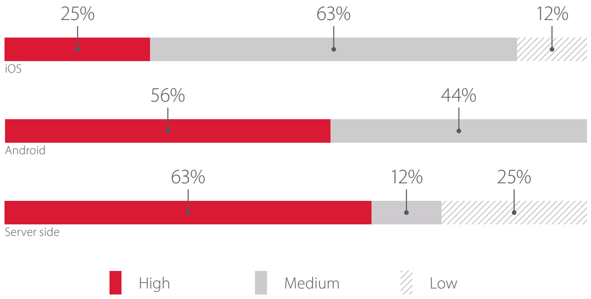
The security level of 8% of mobile banking apps was "acceptable"

In 48 percent of mobile bank apps, at least one critical vulnerability was present. Mobile applications had an average of 0.64 high-severity vulnerabilities—fewer than in online banks.

As compared to 2016, there was a drop in the percentage of high-severity vulnerabilities (from 32% to 29%) and medium-severity vulnerabilities (from 60% to 56%). Correspondingly, the percentage of low-risk vulnerabilities increased, which can be explained by banks' strategy of tackling critical vulnerabilities first.

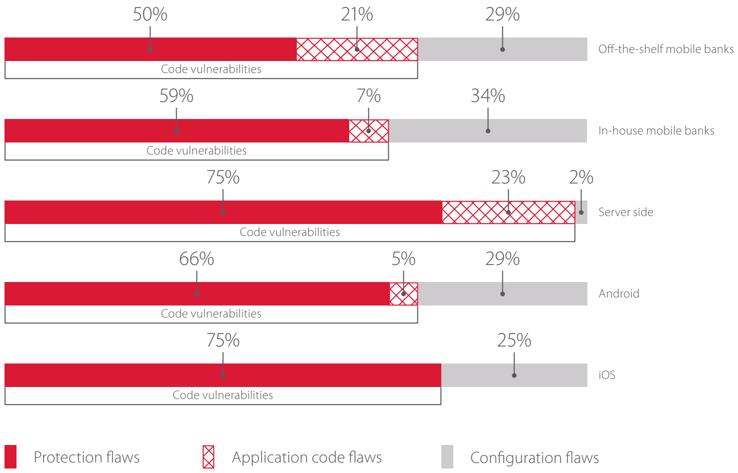


Mobile banking vulnerabilities by severity level iOS apps remain more secure than their Android counterparts

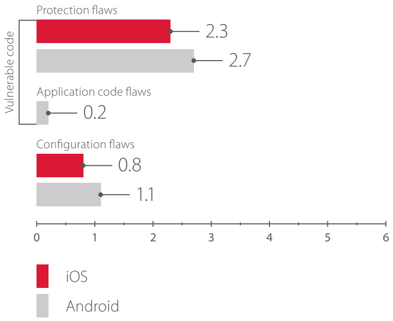


Most severe vulnerability found (percentage of mobile banking applications)

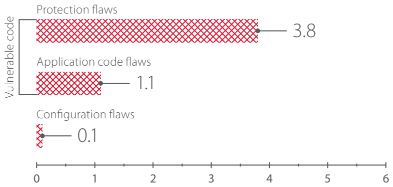
Almost all the mobile banking apps (except for one) were available in both Android and iOS versions, which we analyzed. In some cases, an iOS application did not contain flaws that were present in the Android version.



Vulnerabilities by category



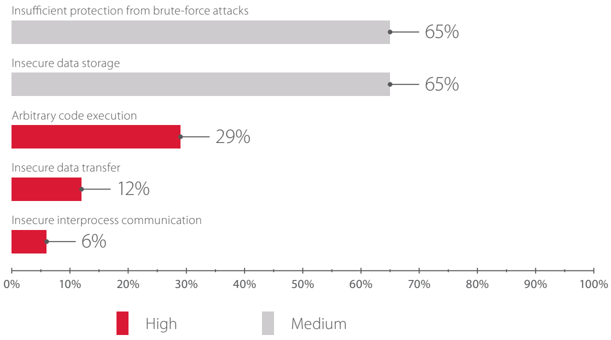
Average number of vulnerabilities on the client side of mobile banks



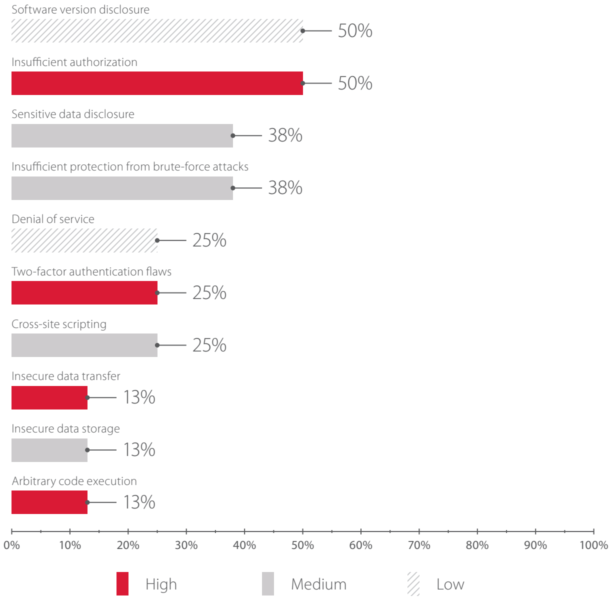
Average number of vulnerabilities on the server side of mobile banks

Most vulnerabilities in mobile applications were caused by flaws in security mechanisms. As already noted, such flaws can also be regarded as code vulnerabilities, but we opted to consider them separately because they emerge at a different stage. Security mechanism flaws occur early in design; code vulnerabilities arise during development.

In 2017, vulnerabilities in mobile application clients were not diverse, so we highlighted only the five most common flaws. Insecure data storage and insufficient protection from brute-force attacks were present in 65 percent of app clients. Intruders can use these vulnerabilities to obtain unauthorized access to user credentials and, subsequently, to the user's account in the mobile bank application. These two types of vulnerabilities can be of either high or medium severity depending on the exploitation context.



Top 5 vulnerabilities on the client side of mobile banks



Top 10 vulnerabilities on the server side of mobile banks

Insufficient authorization remains an acute security issue for the server side of mobile applications. However, the percentage of vulnerable mobile banking apps has dropped from 75 percent in 2016 to 50 percent in 2017.

One common practice is for the user to set a numeric code for accessing a banking application from a mobile device.

However, if no numeric code is set, an intruder can access the mobile banking application. For example, one analyzed application stored a value, which was transmitted with a code for simplified authentication, on the device in cleartext and it could not be changed. Using this value, an intruder can bruteforce the numeric code and access the user's account.

Flaws in two-factor authorization occurred less often in 2017—only in a quarter of mobile application server sides (as compared to half in 2016).

In 13 percent of mobile applications, arbitrary code execution was possible. This vulnerability was typical for the server side of applications. **By exploiting such a vulnerability, an intruder can obtain full control over the server**; execute arbitrary code; read, delete, or change files on the server; escalate privileges, or cause denial of service. Such malicious actions can cause enormous damage to banks' reputation and bottom line.

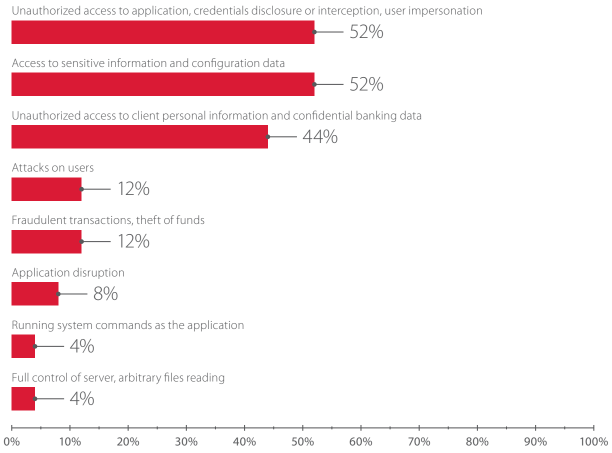
In 52 percent of mobile banking applications, detected vulnerabilities allowed attackers to decrypt, intercept, and bruteforce credentials, or bypass the authentication process entirely. Due to this, attackers could log in to the mobile application as a legitimate user and perform transactions.

In some cases, an intruder, having physical access to a user's device with root access and debugging mode on, can get access to the user's outgoing messages, identifier, and password, and also obtain control over the mobile banking application.

In 44 percent of tested mobile banking apps, detected flaws gave access to clients' banking data. One of the mobile applications had server authorization flaws, which allowed an intruder to get access to user data including names, account balances, deposits, and loans. This not only leads to reputational losses—such information can be used for further attacks.

Attacks on mobile bank applications in 2017 could cause serious harm to both banks and their clients, since most attacks involved:

- User impersonation
- Access to banking data of clients
- Fraudulent transactions



Potential impact of attacks on mobile banks (vulnerable applications)

CONCLUSION

The results of testing in 2017 show that financial applications are becoming increasingly secure. We saw significant improvement in the security of e-banking systems, both in online banking apps and mobile apps. However, many flaws still remain and represent a serious threat for banks and their clients. Clients have private data and banking information at risk. Banks risk losing money and credibility.

As evidenced by years of research, code vulnerabilities are the main cause of security issues in online banking and mobile banking applications. In order to avoid these risks, banks should pay more attention at all stages to proper architecture, careful formulation of technical requirements, and secure development. It is necessary to consider all the subtleties of implementation of security mechanisms, follow SSDLC practices, and rigorously test applications and security mechanisms.

Today, almost every bank assesses application security regularly (at least once per year). Performing source code analysis is also important, especially if the application is based on an off-the-shelf solution, since vendor testing is unable to take all factors of real-world client implementation into account. Perhaps even more important than detecting vulnerabilities, however, is remediating them in a timely manner. This is why after implementing fixes, banks must check to verify that remediation steps have had the desired effect. Eliminating vulnerabilities can take longer than expected. To protect against cyberattacks on online banking apps and the server side of mobile apps, especially while code fixes are in progress, we recommended deploying a web application firewall (WAF).

About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.

POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com