SYNOPSYS®

WHITE PAPER

By the Numbers: Mobile Application Security Risks in Financial Services

To assess the state of mobile application security, the Synopsys Cybersecurity Research Center (CyRC) analyzed more than 3,000 popular Android applications, using Black Duck® Binary Analysis (BDBA). The study explored the most-downloaded and highest-grossing applications across 18 categories and included a targeted analysis of three core areas of mobile application security:

- **Vulnerabilities:** The presence of known software vulnerabilities in an application's open source components
- **Information leakage:** Sensitive data such as private keys, tokens, and passwords exposed in an application's code and configuration files
- **Mobile device permissions:** Applications requiring excessive access to mobile device data and features

For the purposes of this condensed report, we are narrowing the scope of discussion to the CyRC's findings for the mobile applications that power the financial services industry (FSI). Full details of the BDBA results can be found in the report "Peril in a Pandemic: The State of Mobile Application Security."

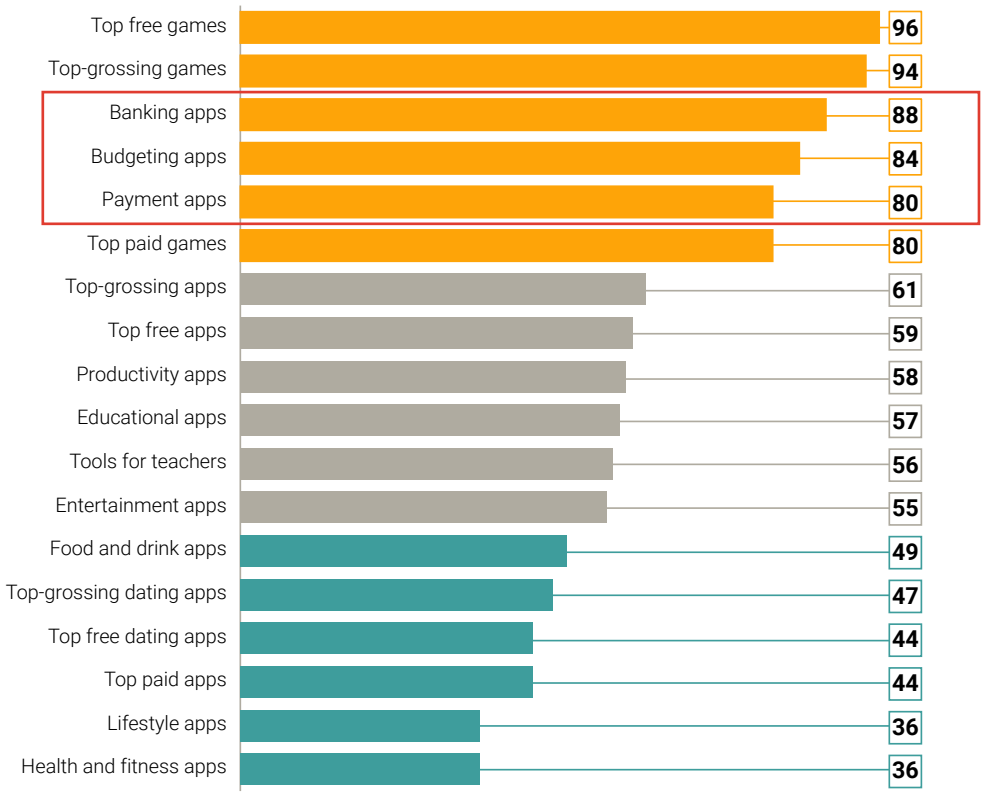
The CyRC's analysis reveals that the majority of applications in use today contain open source components with known security vulnerabilities. Also evident are other pervasive security concerns including sensitive data exposed in the application code and the use of excessive mobile device permissions. These findings were particularly true for the three FSI categories analyzed: payment apps, banking apps, and budgeting apps.

High-level FSI findings

We trust financial applications to be secure because of the sensitive nature of the information they manage and contain. But this trust can be too freely given, the CyRC's findings show.

Of the 3,335 total applications the CyRC scanned, 2,115 contained vulnerable components (63%), with an average of 39 vulnerabilities per vulnerable app. Narrowing the analysis to FSI applications, the numbers are even more concerning.

In analyzing the overall Common Vulnerabilities and Exposures (CVE) data, the most dramatic findings resulted from the analysis of banking applications. Of the 107 banking applications scanned, 94 contained a vulnerability—that's 88%, well above the average of 63%. With a total of 5,179 vulnerabilities identified, the average banking application contained 55 vulnerabilities, denoting them as key application security offenders.



Percentage of scanned apps that contained vulnerabilities, by category

These findings point to the indisputable fact that mobile FSI applications are no more secure than any other type of app.

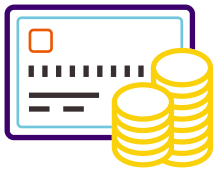
Open source vulnerability findings

When assessing open source security across all categories, the CyRC found that banking apps had the third-highest number of vulnerabilities. This ranking encompasses the highest number of both fixable and nonfixable vulnerabilities, indicating a lack of timely remediation as well as a failure to work toward addressing vulnerabilities with no known fix.

There's much at stake when it comes to financial data; we trust sensitive personal information to these apps. With the implementation of standard security practices and tooling, security teams could easily address almost 40% of the open source vulnerabilities found in this study. Stated differently, nearly 40% of the vulnerabilities identified in our study have an available fix.

In addition, the CyRC's analysis highlights a concerningly high percentage of FSI applications with open source vulnerabilities, and a high number of vulnerabilities per application.

Average number of vulnerabilities per vulnerable application



Payment apps=41

Banking apps=55

Budgeting apps=51

Across all FSI categories, the category with the highest percentage of exploitable vulnerabilities with fixes available was banking at 39%.

Information leakage findings

Put simply, information leakage is when developers accidentally leave personal or sensitive data in the source code or configuration files of the application. Alternately, sometimes developers intentionally leave information in the source code, causing unintentional security implications. In the wrong hands, this information can be used maliciously. The CyRC's findings indicate that popular applications are not free from information leakage. The CyRC examined various key types of information leakage across all applications.

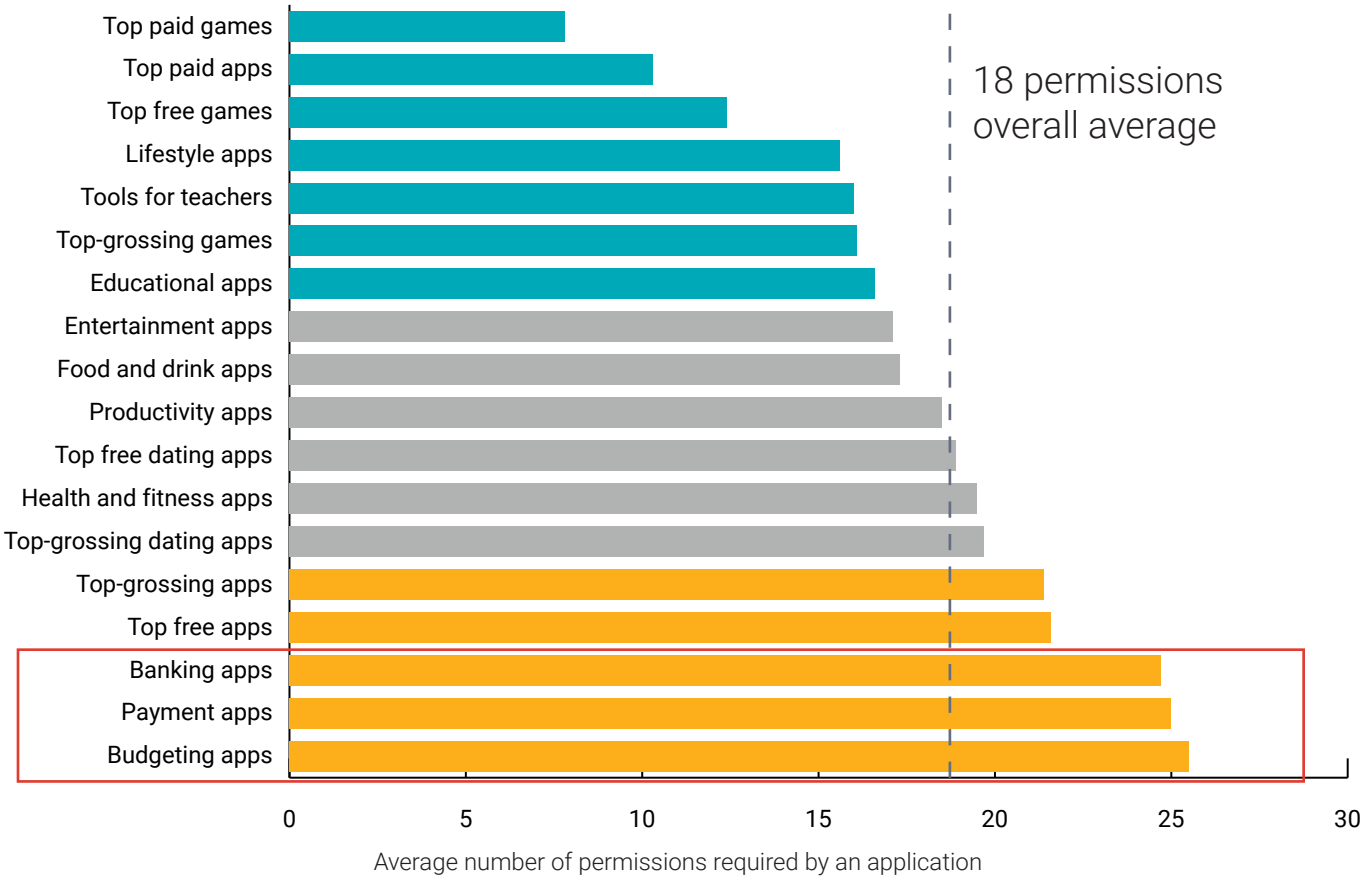
Tokens, keys, and passwords: If developers leave behind this type of information (AWS keys, Google Cloud tokens, user credentials, etc.), it can pose great potential risk. This information allows an individual to access someone's servers, systems, or sensitive properties. From there an attacker can steal IP, plant malware, or launch compute resources that attribute costs to the application owner.

For example, JSON Web Tokens (JWTs) serve as a way to securely pass information between parties. Although these can be encrypted, they often aren't. JWTs require a digitally signed secret key and essentially act as credentials, so they should never be kept longer than absolutely necessary. When left behind in source code, they can be easily decoded to reveal information that helps an attacker exploit the application.

The CyRC found four JWTs in banking apps, and three in budgeting apps—a big cause for concern.

Mobile permissions findings

The CyRC used Black Duck to examine the mobile permissions tied to top Android applications. The team first reviewed the average number of permissions required of a user, per application, both by category and as a whole. The CyRC then looked at specific applications with results that were outside of that average number by more than two standard deviations. Special attention was given to those that asked for significantly more permissions than the average application.



The average number of permissions for all categories was 18. FSI apps had a higher-than-average number of permissions.

- Budgeting apps: 26 permissions on average
- Payment apps: 25 permissions on average
- Banking apps: 25 permissions on average

Key takeaways

The results uncovered by Black Duck Binary Analysis point toward the reality that we should not assume FSI applications are any more secure than applications across other verticals.

Paired with this discovery is the fact that most of the vulnerabilities and risks found in this analysis are either preventable or easily remedied. This lack of remediation can be blamed on a failure to implement robust application security practices and tools.

Solutions like Synopsys Black Duck software composition analysis and Black Duck Binary Analysis keep security teams informed of open source vulnerabilities, potential instances of information leakage, and mobile permissions data. Armed with these tools and the insights they provide, teams can take informed actions and help ensure application security.

To learn more about Black Duck Binary Analysis, visit our website.

To learn more about our complete findings, read the full report, "Peril in a Pandemic: The State of Mobile Application Security."

SYNOPSYS®

The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com