Latin American Journal of Education
www.lajoe.org

ANDROID OPERATING SYSTEM ARCHITECTURE

https://doi.org/10.5281/zenodo.21805259

Erkinov Shohjahan Sherali oglu
Student of TUIT, Cybersecurity facult

Abstract: *Android is the world's most widely used mobile operating system, powering billions of smartphones, tablets, wearable devices, and embedded systems. Its architecture is designed as a layered software stack that provides flexibility, security, and high performance. The Android operating system consists of five main layers: Applications, Application Framework, Android Runtime and Native Libraries, Hardware Abstraction Layer (HAL), and the Linux Kernel. Each layer performs specific functions that ensure efficient communication between applications and hardware resources. The Linux Kernel manages memory, process scheduling, device drivers, and security, while HAL provides standardized interfaces between hardware components and higher software layers.*

Keywords: *Android Operating System, Android Architecture, Linux Kernel, Hardware Abstraction Layer (HAL), Android Runtime (ART), Application Framework, Mobile Operating Systems, Mobile Security, Application Development, Open Source Software.*

Android applications make full use of modern device capabilities, providing users with new technological solutions and convenience. The platform acts as a software environment designed to guarantee the security, integrity and uninterrupted operation of users, stored data, installed applications, devices and network infrastructure.

Keeping an open source platform secure is a complex task that requires a well-thought-out protection system and consistent security measures. Android was built on a multi-layered security system in order to maintain openness and flexibility while being able to reliably protect users of all categories.

Security mechanisms serve primarily to reduce the level of risk for program creators. Professionals with sufficient security experience can freely use the management tools that the system offers and can have confidence in their performance. And programmers who don't care too much about security will be protected by protection pre-configured by the system. Along with providing a stable development environment, Android also offers a number of tools in order to provide additional developer support. Android's specialized security team regularly scans apps vulnerability points and develops recommendations for fixing them. For device manufacturers, which

Latin American Journal of Education
www.lajoe.org

partners with Google, Play Services regularly updates software components that play a key role in protecting network communications, such as OpenSSL. Additionally, the Android SSL testing platform allows developers to detect security gaps that can occur in any given device environment at an early stage [2].

Users have the right to view and control a list of permissions that each app installed on their devices. This approach acts as a barrier against the psychological manipulation techniques that attackers use to persuade device owners to download malicious apps, i.e., social engineering attacks and cyberattacks carried out through third-party apps on the Android system.

The Android system is designed with the principle of minimizing the likelihood of such attacks, and limiting its negative consequences as much as possible in case of success. Even after the device is passed into the hands of the user, the Android security system will improve. Participants in the Android ecosystem — manufacturers, and the general public — say it's important to deliver the necessary fixes in a timely manner for all devices that receive security updates.

Android provides an open source platform and application system for mobile devices. Figure 1.1 shows the security components and describes the different layers of the Android operating system architecture. Each component assumes that the following components are reliably attached. Except for a small amount of Android OS code that works as the root, all code over the Linux kernel is restricted by the application test area.

Device hardware. The Android operating system is capable of working efficiently on a wide range of devices — smartphones, tablets, smartwatches, car multimedia systems, modern smart TVs and game consoles are examples of this. The capability to support various hardware configurations has made the Android system one of the most versatile and widely used mobile platforms on the market. Such flexibility allows developers to create apps for a wide variety of devices within a single platform.

Latin American Journal of Education
www.lajoe.org

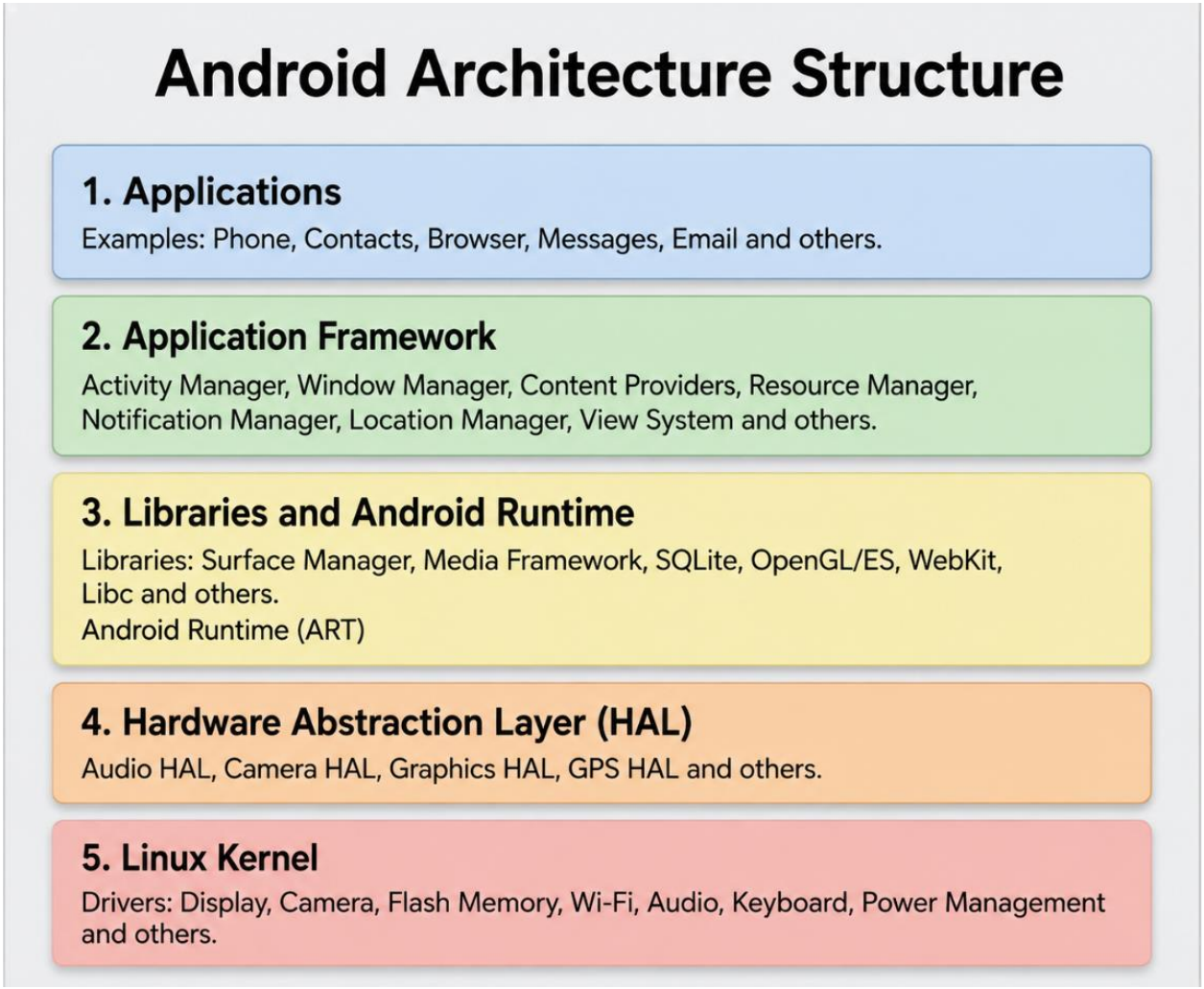

Figure 1.1. Android Layers Structure

The main building blocks of the Android platform are:

Android operating system. The foundation of the system is based on the Linux kernel. All the resources of the device, such as the camera module, GPS navigation system, Bluetooth wireless communication, phone calls and internet connection, are provided to the user exactly through the operating system. It is no coincidence that the Linux kernel should be chosen — it has proven itself in terms of reliability, security, and stability over its decades-long history.

Application Processing Environment. Most Android apps are written in either Java or Kotlin and run in an ART (Android Runtime) environment. However, many applications, especially low-level system services, also use local (native) libraries in order to improve performance speed. Importantly, all applications — both high-end graphics applications and local system services — operate in a single, isolated security environment. Each application has its own dedicated file system area and can only access databases and configuration files within that area. This approach avoids unauthorized data transfer between applications.

Latin American Journal of Education
www.lajoe.org

Android apps enter the system in two different ways:

Pre-installed apps **such as** basic apps such as phone, email client, web browser, calendar, and contacts are delivered with the device. They function as a simple user application and open the standard capabilities of a device to the external environment that other applications can use. Such apps can be available as part of the open Android platform, or they can be made by the device manufacturer separately for their product.

User-Installed Applications — Android provides a free development environment for third-party developers. Through the Google Play Store, users can search for and install hundreds of thousands of different apps on their devices. This openness allows Android ecosystem to continuously evolve, allowing new innovative solutions to emerge [4].

Google Security Services.

For devices that are compatible with Google Mobile Services, Google offers a comprehensive suite of cloud services. While these services aren't officially part of AOSP, they come pre-installed by default on many Android devices around the world and play a key role in ensuring user security.

Key services include:

Google Play **is** a large platform that allows users to search, download, or buy apps for free via device or web browser. In addition, Google Play includes important protection mechanisms, such as automatic scanning of app security, license legality checks, and user community controls.

Android updates — introducing new features and important security patches for select devices — including OTA (over-the-air) — that is, the ability to update a device directly over the network without connecting it to a computer.

Application Services — provides access to modern cloud technologies, such as backing up app data and settings to the cloud and sending push notifications to the device (C2DM).

Application scanning — pre-blocks the installation of malicious applications on the device, and regularly checks for already installed applications. When a dangerous app is detected, it will immediately alert the user or delete it automatically.

SafetyNet **is** a real-time threat detection system while maintaining privacy, which helps Google track known security risks and emerging threats and quickly eliminate them.

SafetyNet Attestation **is a** third-party API service that independently verifies a device's compliance with CTS (Compatibility Test Suite) requirements. It allows you to verify not only the authenticity of the device itself, but also the Android application that's been linked to the system.

Android Device Manager is an important security tool that allows you to determine the location of a lost or stolen device by using a web interface or a

Latin American Journal of Education
www.lajoe.org

special application, and if necessary, remotely lock your device or delete its data.

Overall Security Program Structure

The Android security system encompasses several interrelated strategic areas, and each of these areas serves to strengthen the overall level of protection of the platform:

Safety at the design stage. Protection measures are taken into account from the very first design stage — a large-scale and flexible security model is developed. Each core functionality is reviewed jointly by software engineers and security industry mature experts, while defense mechanisms are seamlessly and organically incorporated into the system architecture.

Penetration Tests and Code Analysis. Throughout the development process, both Android code and its included open source components are subjected to strict and comprehensive security audits. This work will be done jointly by the Android security team, Google security engineers, and external independent experts. The main goal is to identify all vulnerabilities and pre-model the analysis methods used in real-world attacks before the official version is released.

Open source and team control. The composition of the AOSP allows any stakeholders to conduct an in-depth independent security audit. Android relies on open-source components that have been tested by the independent community, much like its Linux kernel. And the Google Play platform provides an open space for users and organizations to share ideas about the quality and security of apps.

Insider Management. Despite all preventive measures, safety issues may arise even after the product is released. Therefore, Android team has developed a comprehensive and fast response system. Security experts continuously monitor the software community, discussing potential vulnerabilities, and conducting in-depth analysis of identified security flaws. Once the issue is confirmed, prompt action is taken to mitigate the threat to all users as much as possible: an AOSP update, removal of the problematic app from the Google Play Store, or remote removal from distributed devices.

Monthly security updates. Google's Android security team regularly publishes a set of updates every month for Google's own devices and all partner device manufacturers. This practice serves to keep users in a state of constant protection against new threats [6].

Platform Security Architecture

Android aims to achieve the following three main goals by adapting the protection of the traditional operating system to the requirements of the modern mobile environment:

1. securely store the application and user personal data from unauthorized access;
2. prevention of misuse of network and system resources;

Latin American Journal of Education
www.lajoe.org

3. guarantee complete logical separation of applications from both the system and the core of the system.

a. To accomplish these strategic goals, Android provides the following key security mechanisms and tools:

4. An operating system-level multi-layered and robust protection system, built on the Linux kernel;

5. a sandbox mechanism that is enforced on all third-party and system applications;

6. a protocol for information exchange, which is carried out securely and controllably between the various processes;

7. signing mechanism designed to verify the authenticity of applications and guarantee that they have not been tampered with;

8. A permissions management system that is clearly declared by the app and consciously approved by the end user.

Current threats and vulnerabilities in Android OS

The rapid development of digital technology is also having a major impact on the mobile application market. By the end of 2018, the number of mobile application downloads by users exceeded 200 billion times. Looking at the results of the Digital Engagement Survey, more than 57% of the total time people spend online has been spent using apps on smartphones or tablets.

Today, mobile devices have become an integral element of everyday life: social networks and instant messengers, online banking, corporate management systems, personal cabinets of a mobile operator — modern people use them almost every day. Juniper Research Center estimates that the number of users using mobile banking services is approaching the two billion mark, which is about 40% of the world's adult population.

Experts from the security company Positive Technologies regularly check and analyze the protection of mobile applications. The statistics collected during testing applications for iOS and Android platforms in 2018 yielded the following important conclusions.

Vulnerabilities rated as high-level threats were detected in 38% of iOS apps and 43% of Android apps.

Most of the security flaws are the same feature for both platforms. The issue of keeping user data safe was highlighted as the most common vulnerability and it was noted in 76% of the scanned applications. Information that can be at risk includes access passwords, payment details, personal identification information, and correspondence history.

Of particular concern is the fact that 89% of the vulnerabilities identified can be exploited remotely using malware,

Latin American Journal of Education
www.lajoe.org

even if an attacker does not have physical access to the user's device [5].

The bulk of the shortcomings can be found in incorrect implementation of security mechanisms: for iOS apps, the scorescore is 74%, for Android apps 57%, and 42% for server parts. These types of vulnerabilities often appear at the architecture stage, and their elimination requires major changes to the entire codebase.

Client-side vulnerability analysis

60% of all detected vulnerabilities indicate that they are concentrated in the user side of the application. Of these, 89%, direct physical access to the device is not necessary for use. And more than 56% of vulnerabilities can be exploited without administrative permissions — i.e., without jailbreaking or rooting.

The incidence of critical vulnerabilities in Android apps is slightly higher than in iOS: 43% vs. 38%. However, this difference isn't really that big and the overall level of protection of the client parts of the apps on both platforms can be estimated to be almost equal. For both systems, a third of the client-side vulnerabilities are classified as high-risk, indicating the need to fundamentally rethink the approach to security in mobile applications.

Latin American Journal of Education
www.lajoe.org

Figure 1.2. Maximum level of vulnerability risk (specified as percentage of client-side parts)

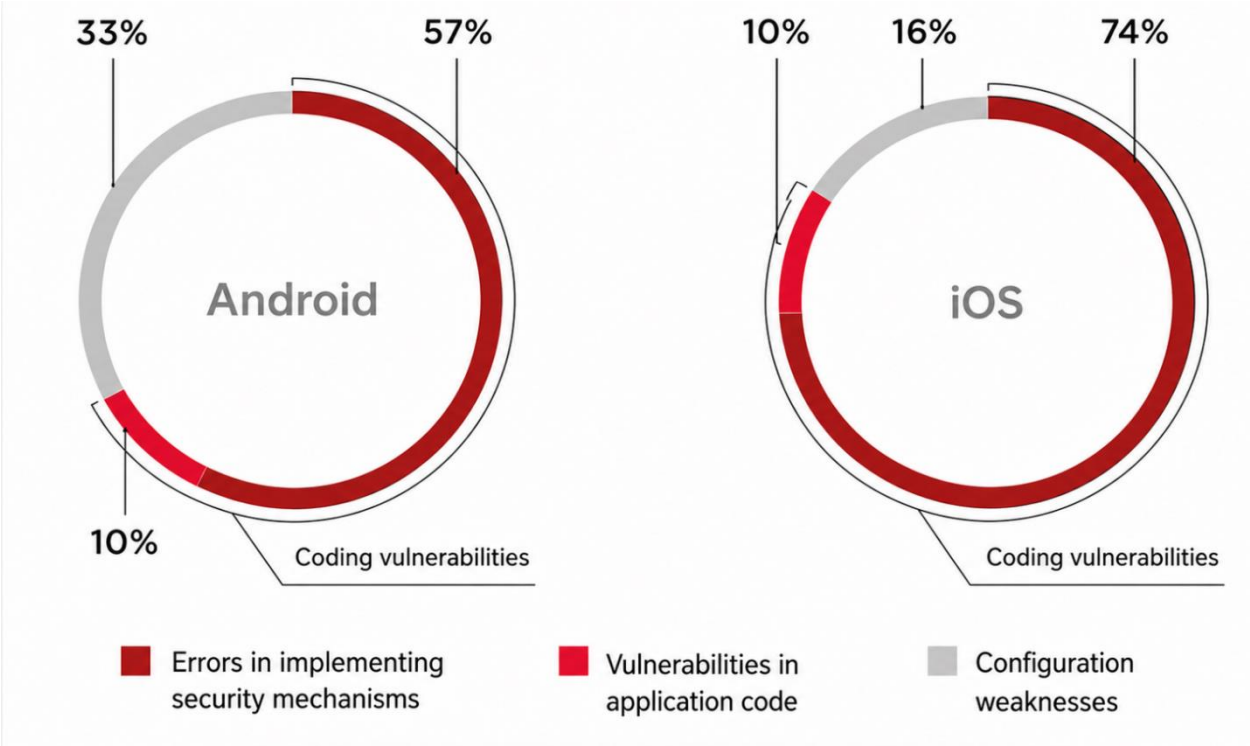

Figure 1.3. Ratio of different levels of risk vulnerabilities

Latin American Journal of Education
www.lajoe.org

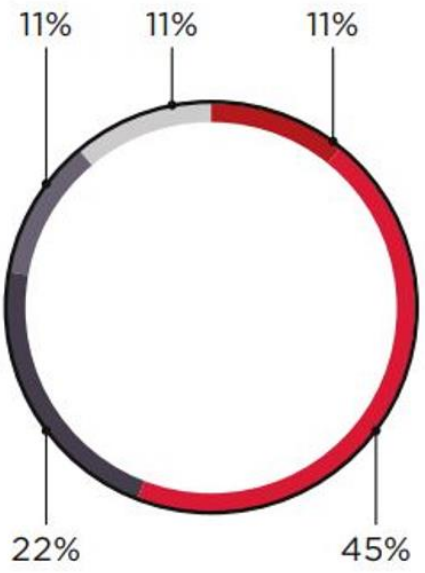

Figure 1.4. Security level of client parts (as a percentage of systems)

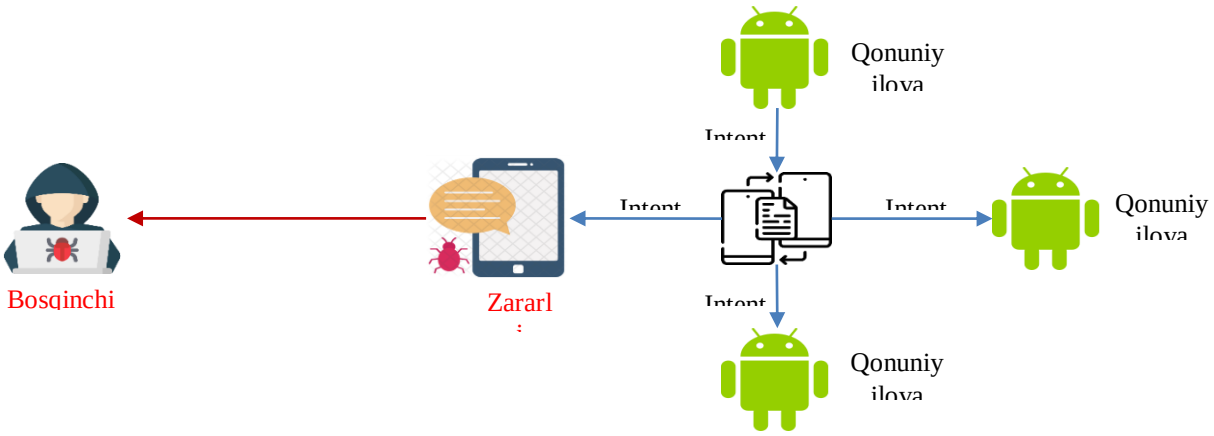

Figure 1.5. Secure inter-process connection scheme within Android operating system

A vulnerability in dangerous inter-process communication is introduced during the design phase of interfaces for interaction between application components and refers to errors in the implementation of security mechanisms. Bugs in security mechanisms caused 74% of vulnerabilities in iOS apps and 57% of vulnerabilities in Android platforms.

Latin American Journal of Education
www.lajoe.org

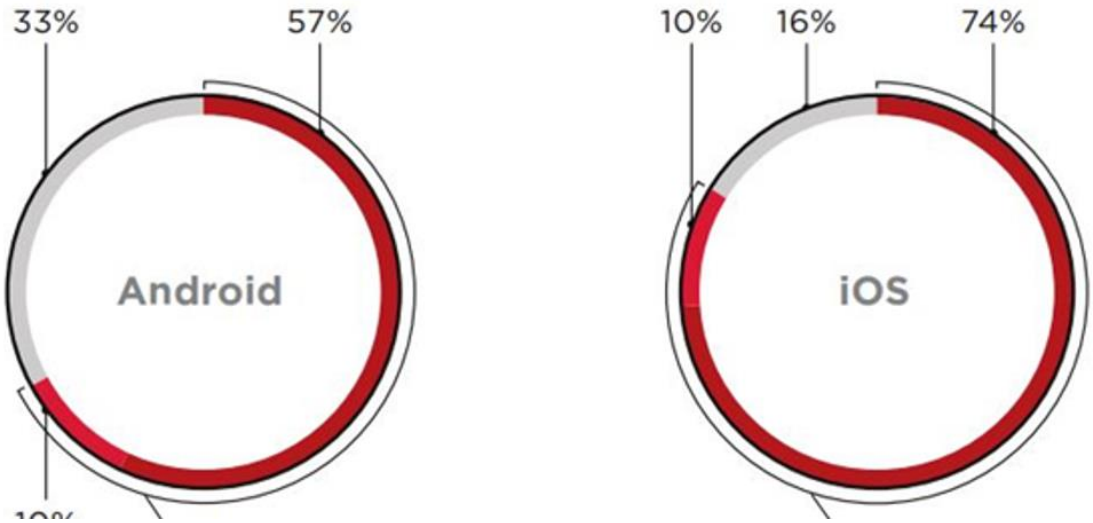

Figure 1.6. The proportion of weaknesses of various types

Modern mobile devices store innumerable types of data, such as user location, personal identifiable data, private correspondence, service account details, and financial transaction history. However, insufficient attention is often paid to how securely this information is stored within applications. In the OWASP Mobile Top 10−2016 ranking, the problem of insecure data storage ranks second, and this vulnerability was detected in 76% of the mobile applications examined.

Real-life examples vividly illustrate how serious this risk is. In August 2018, Air Canada Airlines' mobile application was cyberattacked, as a result of which the personal data of more than 20 thousand users fell into the hands of attackers. According to statistics from McAfee, the number of malware intended for mobile devices is growing rapidly from year to year: from 1,5 million to 2 million new malware samples are detected every quarter, and by the end of 2018 their total number exceeded 30 million. This rapid increase in malware is making client-side attacks an increasingly common phenomenon, while server-side vulnerabilities are losing their primary threat status.

There are various flaws in the server parts of mobile applications, both in the application code and in the security mechanisms. In particular, it is not uncommon for two-factor authentication to be implemented incorrectly. So, in particular, when two identical requests are sent to the server in a row and with a minimum interval, a one-time password will be sent to the user both via push notification and SMS at the same time. In this case, an attacker who can intercept SMS messages might be able to perform transactions — for example, financial transfers — on behalf of a legitimate user.

Conclusion

The Android operating system architecture provides a robust, scalable, and modular platform for modern mobile devices. Its layered design enables efficient interaction between applications

Latin American Journal of Education
www.lajoe.org

and hardware while maintaining security, reliability, and performance. The Linux Kernel ensures stable hardware management, the Hardware Abstraction Layer simplifies hardware communication, Android Runtime optimizes application execution, and the Application Framework provides essential services for software development. The open-source nature of Android encourages innovation and allows manufacturers and developers to customize the operating system for different devices and applications. Understanding Android architecture is essential for mobile application developers, cybersecurity specialists, and researchers because it provides the foundation for creating secure, efficient, and high-performance mobile applications.

REFERENCES:

1. Android Developers. (2025). *Android Platform Architecture*. https://developer.android.com

2. Android Open Source Project (AOSP). (2025). *Platform Architecture*. https://source.android.com

3. Meier, R. (2023). *Professional Android*. Wiley Publishing.

4. Burnette, E. (2022). *Hello, Android: Introducing Google's Mobile Development Platform*. Pragmatic Bookshelf.

5. Yaghmour, K. (2013). *Embedded Android*. O'Reilly Media.

6. Ye, R. (2017). *Android System Programming*. Packt Publishing.

7. Levin, J. (2014). *Android Internals: A Confectioner's Cookbook*. Technologeeks Press.

8. Silberschatz, A., Galvin, P. B., & Gagne, G. (2018). *Operating System Concepts* (10th ed.). Wiley.