Abstract der fertigen Arbeit

Smartphone apps have become deeply integrated into our daily lives. Approximately 6.9 billion smartphone users worldwide relied on more than 8.9 million apps in 2023. Users employ these apps to manage communication, finances, and health data. Consequently, they must trust that the apps are developed securely and handle their personal data responsibly. However, modern apps rarely operate in isolation. Instead, they interact with the mobile operating system, cloud backends, or Internet of Things (IoT) devices, and each interaction expands the attack surface because the security of the overall system depends on its weakest link. Beyond direct communication partners, the resources used during the development process, e.g., its software supply chain, can be seen as part of the mobile app ecosystem, further extending the attack surface.

In this thesis, we identify weak links in the mobile app ecosystem, develop large-scale analyses to uncover security and privacy issues, and responsibly disclose our findings to improve the security and privacy of the ecosystem. To this end, we analyze four components: First, we study the communication behavior of IoT companion apps. Second, we analyze the iOS local network permission from both a technical and a user perspective. Third, we study secrets embedded in apps, ranging from tokens required for online services to secrets unintentionally included during development. Finally, we analyze the security of iOS dependency management systems to uncover software supply chain threats.

Overall, we uncover various security and privacy issues, for example, Message Queuing Telemetry Transport (MQTT) brokers allowing unauthenticated access, techniques that allow bypassing the iOS local network permission, leaked functional credentials in mobile apps, and supply chain vulnerabilities that affect popular apps from well-known companies.