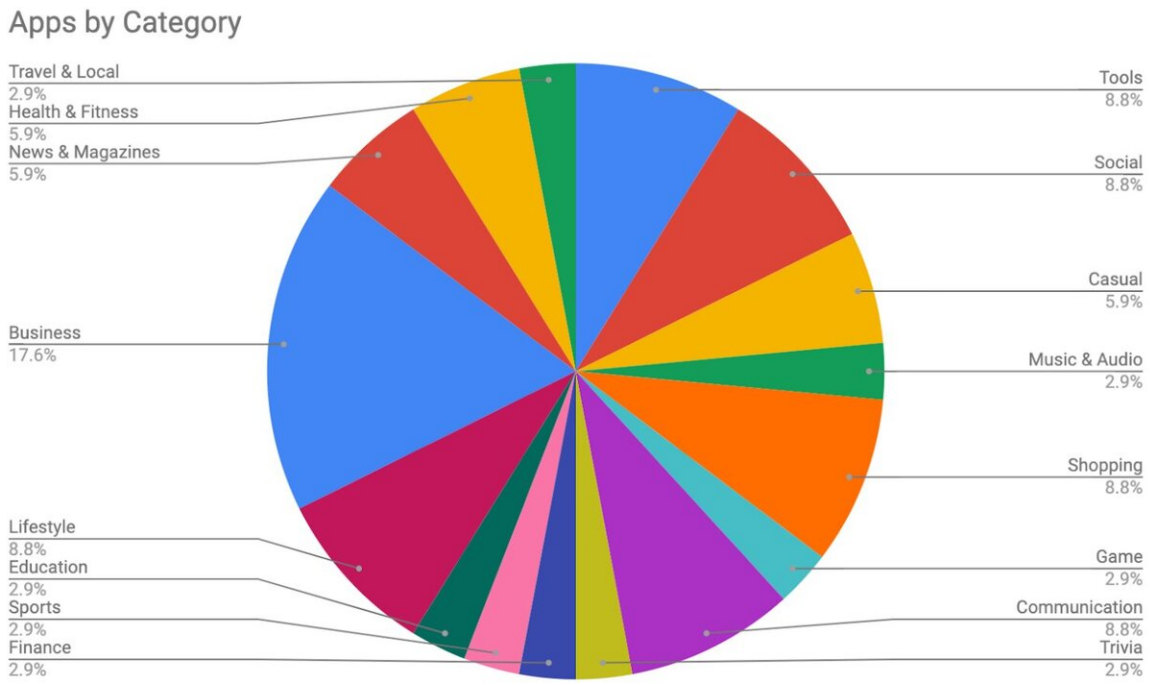
Unsecured cloud configurations expose data across thousands of mobile apps

March 8 2021, by Sarah Katz



Mobile App Risk Chart. Credit: Zimperium

In mobile application development, server-side storage of the application's data remains top priority. In particular, many developers have begun using backend APIs that enable their apps to query a server for information in real time rather than reply upon static data stored in files. However, as many cloud storage services have been found to use

unsecured configurations, data on thousands of mobile applications could be at risk.

A main challenge arises when the task of securing the configurations of these services falls upon the app developers rather than the provider, such as Amazon AWS, Google's Firebase Storage or Azure by Microsoft. When developers use these storage services for the very purpose of having their API security taken care of, they invest the majority of their efforts into building the apps rather than protecting stored information. Such an oversight could threaten many app developers as well as their employers and users.

In 2021, the mobile security company Zimperium found that over 14 percent of mobile apps using cloud storage face risks due to unsecured configurations. This research has revealed that, globally and across all industries, various apps are vulnerable to the exposure of publicly identifiable information (PII), fraud and unregulated internal IP/configuration sharing.

Because the security of these mobile apps tends to reply on the cloud provider's default settings, the developer might not even realize data exposure could be occurring. In fact, even when cloud providers offer developers security guidelines, the developers might not adhere to them.

With PII exposure, all manner of personal medical data, game apps, social media apps and fitness apps are put at risk. In terms of fraud enablement, such exposure provides attackers access to user data on mobile ecommerce platforms, transportation apps, gambling apps and payment information for Fortune 500 mobile wallet. Finally, entire IPs and systems face the threat of malicious data alteration with major music apps, major news services, Fortune 500 software companies, major airports and major hardware developers.

Overall, the vertical most impacted by unsecure cloud server configurations appears to be business, at 17.6 percent risk. In order to mitigate such risks, developers can begin by ensuring that the cloud storage database they are using is unaccessible from outside interference. Furthermore, developers can prioritize a secure software development lifecycle in order to prevent execution of unsanitized code.

At the end of the day, the challenge of mobile application security remains largely with the app developers themselves. While some organizations might shy away from more widescale changes such as patching always-on systems or replacing vulnerable hardware, app creators alone can help prevent many threats. Once more developers embrace this responsibility, securing mobile apps can become a norm rather than an afterthought.

More information: Newman, L. H. "Thousands of Android and IOS Apps Leak Data From the Cloud." Wired, Conde Nast, 8 Mar. 2021, www.wired.com/story/ios-android-leaky-apps-cloud/

Tamir, C. "Unsecured Cloud Configurations Exposing Information in Thousands of Mobile Apps." Zimperium Mobile Security Blog, Zimperium, 8 Mar. 2021, blog.zimperium.com/unsecured-c … ands-of-mobile-apps/