**Interdependent privacy in third-party app platforms**

**by Shuaishuai Liu and Gergely Biczok**

**{sliu,biczok}@crysys.hu**

We propose to discuss **interdependent privacy issues plaguing third-party application platforms via their permission systems.** Third-party application platforms use permission management mechanisms to explain to users how to access and transfer data, while expecting to use data flexibly within the scope of users' permission to enhance user experience. The core mechanism of the permission system of third-party application platforms is that the system asks the user whether she agrees to transferring and processing data within the scope of the permission description. Still, this mechanism cannot deal with the problem that i) data managed by this user may involve others, and ii) does not/cannot obtain the consent/authorization of others, giving rise to interdependent privacy issues [1]. For example, if the permission “access photos in your album” is obtained from the installing user, the system can reasonably obtain the photos, even if they contain the likeliness of other natural persons/users.

We studied the permission systems of and scraped data from several third-party application platforms [2], including Google Play Store, Mozilla extension, Opera extension, Google Workspace and Zoom Marketplace. These datasets contain numerous different application categories, the number of users, ratings, and types of permissions requested from users.

We classify permissions into three pre-defined categories: invoking interdependent privacy (IDP), potentially invoking interdependent privacy (PIDP), and not invoking interdependent privacy (NIDP). If a permission directly enables access to private data related to a natural person other than the user herself, it is in IDP; e.g., the READ\_CONTACTS permission in Android. If a permission potentially enables access to private data related to a natural person other than the user herself, it is in PIDP. Such risk can be realized through i) accessing data that may implicate multiple parties, such as photos or documents (e.g., READ\_EXTERNAL\_STORAGE in Android); ii) enabling a restricted action that may create multi-party data, such as photos or audio recordings (e.g., RECORD\_AUDIO in Android); and iii) enabling inference of other’s private data with reasonable effort, such as location via co-location information from other sources (e.g., ACCESS\_FINE\_LOCATION in Android). Note that granting a PIDP permission does not automatically constitute privacy loss for a third party; the loss is context-dependent and may require additional effort from the app developer or an adversary. If a permission does not belong either to IDP or PIDP, then it is in NIDP, and not in our focus.

By analyzing these datasets, we found that each platform has many IDP permissions and many applications requesting IDP permissions. We also found that some applications in categories such as communication and business clearly request more IDP/PIDP permissions from users.

The responsibility for managing interdependent privacy risks should not be borne by the user, from the perspective of the platform, application, and service provider; see the 3R principle (realize there is a data transfer, realize others' rights and respect others' rights) [3], a brief description of some potential solutions is given here.

**Transparency**: The first two aspects relate to transparency, by classifying and describing permissions in detail, such as classifying permissions into IDP/PIDP/NIDP, improving users' awareness of the interdependence of data. Note that Zoom Marketplace's permission system does this to some extent; they classify permissions as " Associated with you" and "Associated with you and others you're allowed to access", which allows users to realize that the data is only their own or also concerns others. We did not find such descriptions explicit in the permission systems of other platforms.

**Risk avoidance**: After giving a specific description of the scope of the permission, the platform could give the user the right to disable the permission, even if disabling certain permissions will affect user experience negatively. Ideally, the platform and the app should provide a joint solution to such problems (app should be constructed in a way to allow for suppressing IDP permissions). So far, many third-party application platforms adopt the mechanism of “all or nothing”, i.e., the user agrees to grant the application permission, then installs and uses it; or cannot use it at all.

**Control**: For risks arising from certain IDP issues, it is difficult to solve only by a simple permission system, many mature technologies, such as image recognition and text matching, can provide some technical solutions, for example, image recognition can filter out the private information involving others when users share visual data. We are currently doing research in this area.

[1] G. Biczók and P. H. Chia. "Interdependent privacy: Let me share your data." *International conference on financial cryptography and data security*. Springer, Berlin, Heidelberg, 2013. URL: <https://fc13.ifca.ai/proc/10-1.pdf>

[2] S. Liu, B. Herendi, and G. Biczók. "Interdependent privacy issues are pervasive among third-party applications." *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, Cham, 2021. 70-86. URL: <https://www.crysys.hu/publications/files/LiuHB21dpm.pdf>

[3] B. Kamleitner and V. Mitchell. "Your data is my data: a framework for addressing interdependent privacy infringements." *Journal of Public Policy & Marketing* 38.4 (2019): 433-450. URL: <https://research.wu.ac.at/ws/portalfiles/portal/18609500/0743915619858924.pdf>

Bio1: Liu is a PhD student in the the CrySyS Lab at the Budapest University of Technology and Economics (BME). His research focuses on the data privacy, cybersecurity.

Bio2: Gergely Biczok is an associate professor in the CrySyS Lab at the Budapest University of Technology and Economics (BME). Previously, he was a postdoctoral fellow at the Norwegian University of Science and Technology, a Fulbright Visiting Researcher to Northwestern University and a research fellow at Ericsson Research. His research focuses on the privacy, security, and economics of networked systems. His pet topic is interdependent privacy.