RAICC: Revealing Atypical Inter-Component Communication in Android Apps

Jordan Samhi*[1]

[1]Université du Luxembourg (TruX) – Luxembourg

Résumé

La communication entre les composants (ICC) est un des mécanismes les plus importants dans les applications Android.
En effet, il permet aux développeurs de mettre en place de riches fonctionnalités et la réutilisation des composants entre les applications.
Bien que ce mécanisme rende la modélisation des applications Android difficile, des approches ont été développées (e.g., EPICC, ICCTA, AMANDROID, etc.) pour améliorer les analyses statiques d'applications Android en se concentrant sur les méthodes documentées (e.g., startActivity).
Dans ce travail nous montrons que les modèles existants sont incomplets car le framework Android possèdent d'autres méthodes atypiques pour effectuer de la communication entre les composants.
Nous proposons de récupérer systématiquement ces méthodes atypiques, ainsi qu'une approche statique, RAICC, pour la modélisation de nouveaux liens ICC pour booster les analyses existantes. Nous montrons que RAICC améliore la précision et le rappel des outils existants permettant de détecter des fuites de données dans des applications de benchmark.
De plus, nous montrons empiriquement que les méthodes ICC atypiques sont largement utilisées dans les applications Android.
Enfin, nous montrons que RAICC augmente le nombre de liens ICC trouvés de 61,6 % dans des malware, et que RAICC permet la détection de potentielles nouvelles vulnérabilités ICC

*Intervenant