

Titre:

Analyse hybride du code pour détecter les violations de la confidentialité dans le système Android.

Résumé :

La sécurité dans les systèmes Android exige une protection des données privées manipulées par les applications tierces. Ces applications peuvent provoquer la fuite des informations confidentielles sans l'autorisation de l'utilisateur.

Certains mécanismes utilisent des techniques d'analyse dynamique basées sur le "data-tainting" pour suivre les flux d'informations et pour protéger les données sensibles dans les smartphones. Mais ces techniques ne propagent pas la teinte à travers les flux de contrôles. Cela peut provoquer un problème d'undertainting. En particulier, les applications malveillantes peuvent contourner le système Android et obtenir des informations sensibles à travers les flux de contrôle en exploitant le problème d'undertainting. Mes travaux de recherche portent sur l'analyse hybride du code pour contrôler la manipulation des données privées par les applications tierces qui exploitent les flux de contrôle pour obtenir des informations sensibles. L'approche proposée résiste aux attaques d'obfuscation de code et aux attaques par canaux cachés reposant sur les dépendances de contrôle pour obtenir des informations sensibles dans le système Android.