Towards trustworthy detection and prevention of threats for mobile devices

Améliorer la confiance dans la détection et la prévention des menaces sur les équipements mobiles

Mots clés :
● Directeur de thèse : refik MOLVA
● Co-encadrant(s) :
● Unité de recherche : Laboratoire de recherche d'EURECOM
● Ecole doctorale : École Doctorale Informatique, Télécommunications, Électronique de Paris
● Domaine scientifique principal: Sciences et technologies de l'information et de la communication

Résumé du projet de recherche (Langue 1)

The importance of mobile phones in our everyday life has increased significantly during the last decade, and a number of security sensitive operations are already often performed by means of a mobile phone. This PhD thesis aims at addressing the open problems of the state of the art of malware analysis for mobile phones. This work will aim at developing a generic and comprehensive framework capable of performing behavioural malware analysis for mobile systems, and a set of analysis implemented on top of the aforementioned framework which leverage both static and dynamic techniques to trigger and record malicious behaviors in unknown applications. One of the main focus will be to provide transparency to the framework, so that the applications under analysis cannot detect and circumvent the analysis. The framework will also be able to perform holistic analysis, giving the same importance to each of the components within an application and the interactions between them. In addition, a shrunken version of the framework could be deployed on end-user’s mobile devices in order to perform real-time malware analysis and protection, leveraging malicious behaviour recognition.