Demonstrating the Effectiveness of MOSES for Separation of Execution Modes

Giovanni Russello*, Mauro Conti†, Bruno Crispo‡, Earlence Fernandes∓, Yury Zhauniarovich‡

* University of Auckland, New Zealand † University of Padua, Italy ‡ University of Trento, Italy ∓ University of Michigan, USA (work done at Vrije Universiteit Amsterdam)

Motivation
- Same device multiple usage (e.g. BYOD policy)
- Need to separate sensitive corporate data from personal one
- Avoid energy demanding (para)virtualizations (Trango, VirtualLogix, L4 microkernel, L4Android)

MOSES Idea and Features

Main idea: separate security Profiles (SP); applications replicated in one SP cannot access data in other SPs.

Features:
- Separation of application data between different profiles
- Ability to have fine-grained policy
- Compatible with existed applications
- Security Profiles can be activated automatically and manually

MOSES Architecture

Security Profile change

Moses Security Profiles can be changed:
- Automatically (by the system based on Contexts assigned to SP)
- Manually (using MosesSpChanger application)

Steps:
- Specify name, default rule and priority
- Assign allowed applications
- Assign Special Rules
- Assign Contexts

Moses Special Rule configuration

Steps:
- Specify the name of Special Rule
- Select rule type (action)
- Select fine-grained operation
- Enter target of the rule
- (Optional) Enter perform action

Moses operation

(a) All applications allowed

(b) Camera, Gallery, Messaging, Music applications not allowed

Figure 5: Main window of Launcher application