Demonstrating the Effectiveness of MOSES for Separation of Execution Modes

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

∗ University of Auckland, New Zeland † 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)virualizations (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

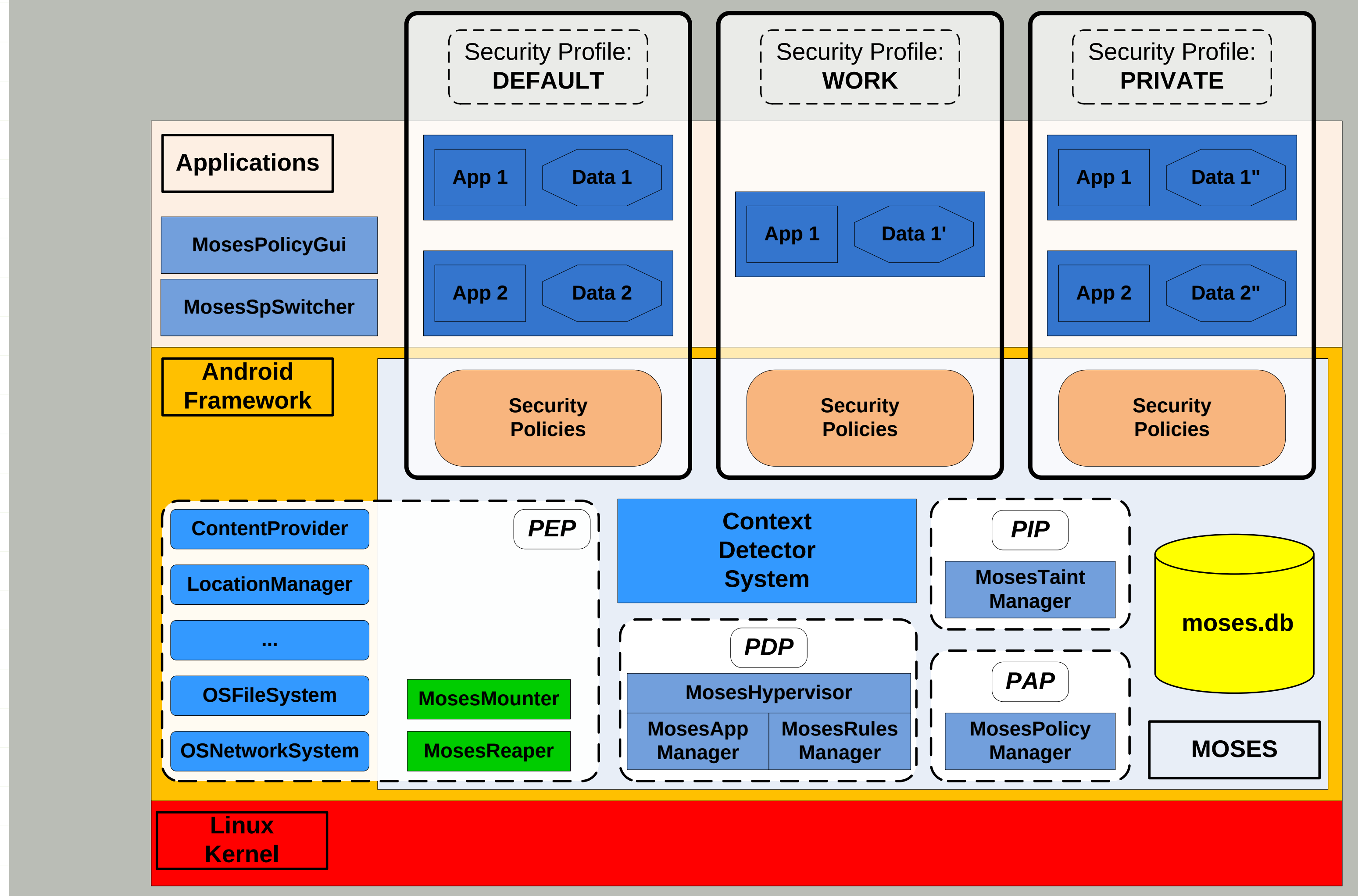
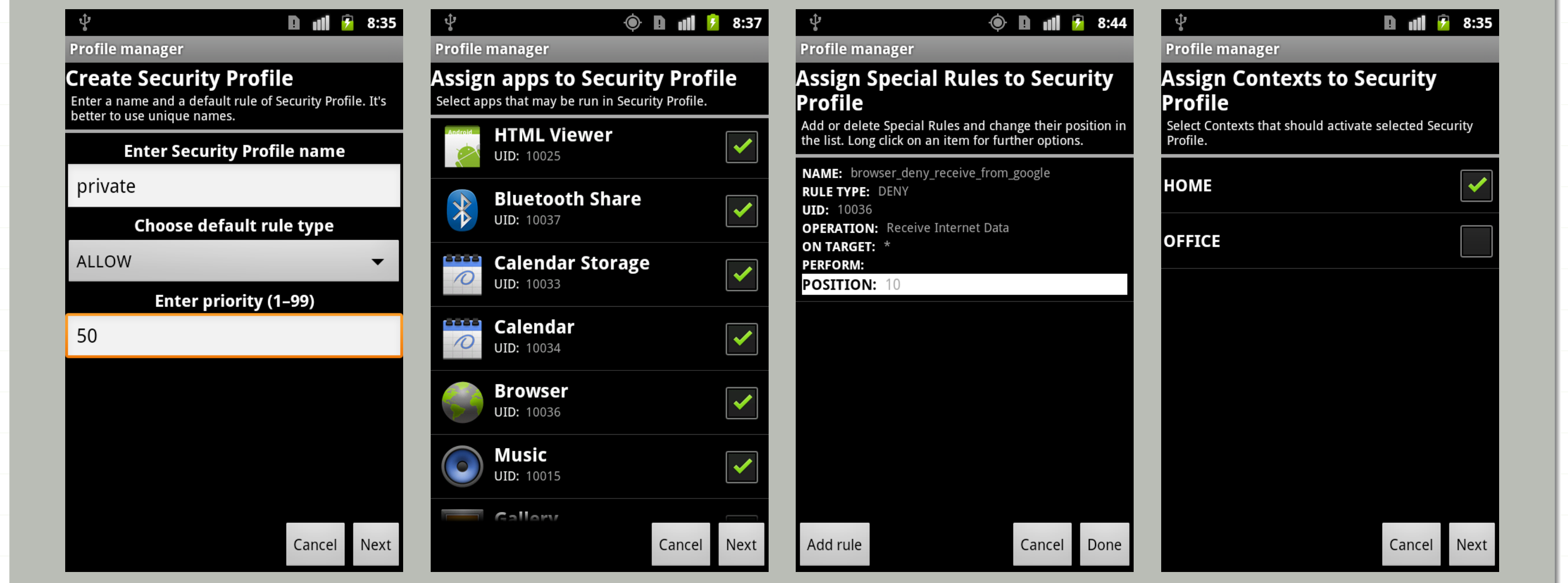


Figure 1: MOSES Architecture

MOSES Security Profile configuration

Steps:

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



8:35
Profile manager
Create Security Profile
Enter a name and a default rule of Security Profile. It's better to use unique names.
Enter Security Profile name: private
Choose default rule type: ALLOW
Enter priority (1–99): 50
Cancel Next

(a) Name, default rule type and priority configuration

8:37
Profile manager
Assign apps to Security Profile
Select apps that may be run in Security Profile.
HTML Viewer UID: 10025 ☑
Bluetooth Share UID: 10037 ☑
Calendar Storage UID: 10033 ☑
Calendar UID: 10034 ☑
Browser UID: 10036 ☑
Music UID: 10015 ☑
Gallery
Cancel Next

(b) Selection of allowed applications

8:44
Profile manager
Assign Special Rules to Security Profile
Add or delete Special Rules and change their position in the list. Long click on an item for further options.
NAME: browser_deny_receive_from_google
RULE TYPE: DENY
UID: 10036
OPERATION: Receive Internet Data
ON TARGET: *
PERFORM:
POSITION: 10
Add rule Cancel Done

(c) Assignment of Special Rules

8:35
Profile manager
Assign Contexts to Security Profile
Select Contexts that should activate selected Security Profile.
HOME ☑
OFFICE □
Cancel Next

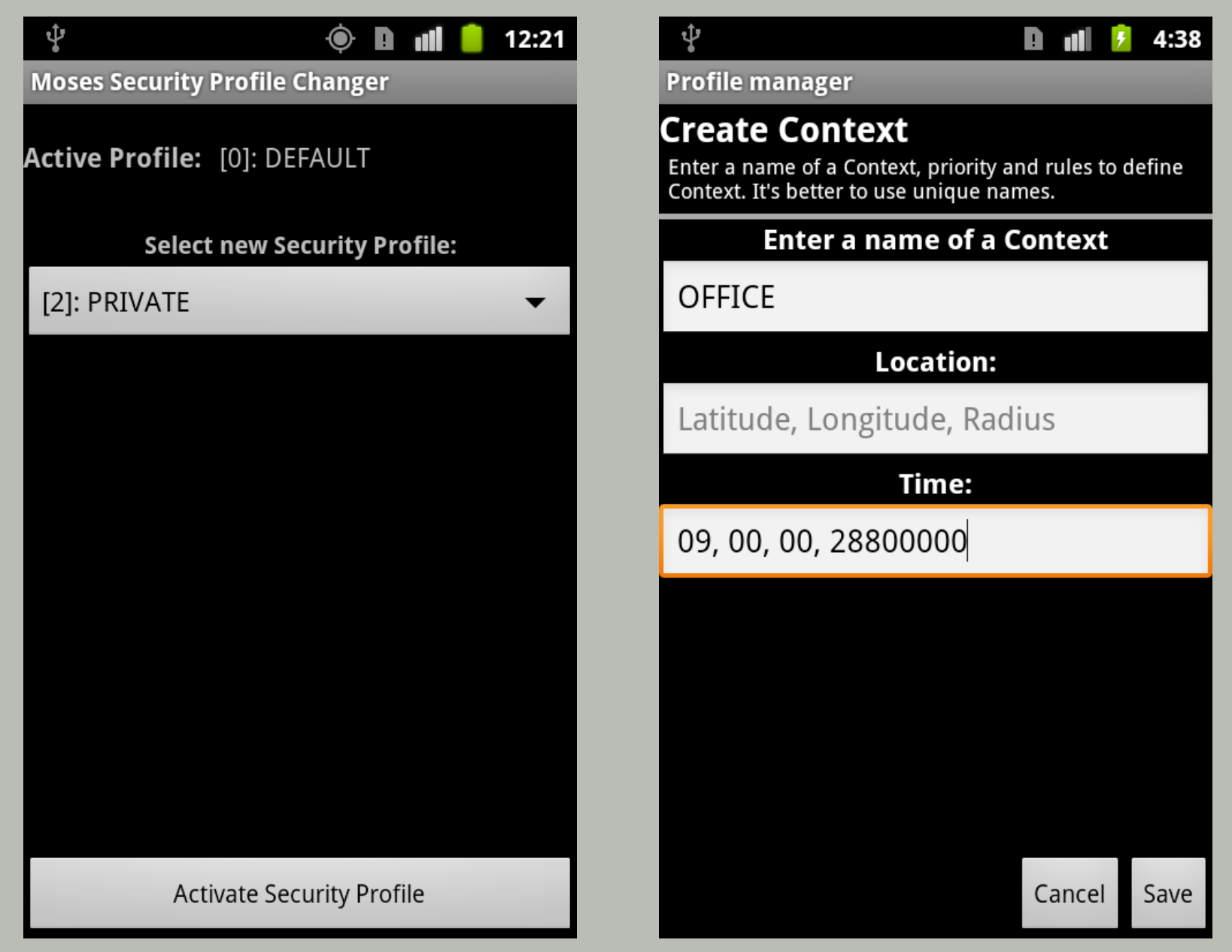
(d) Context assignment

Figure 2: Moses Security Profile configuration

Security Profile change

Moses Security Profiles change be changed:

- Automatically (by the system based on Contexts assigned to SP)
- Manually (using ***MosesSpChanger*** application)



12:21
Moses Security Profile Changer
Active Profile: [0]: DEFAULT
Select new Security Profile: [2]: PRIVATE
Activate Security Profile

(a) MosesSpChanger main window

4:38
Profile manager
Create Context
Enter a name of a Context, priority and rules to define Context. It's better to use unique names.
Enter a name of a Context: OFFICE
Location: Latitude, Longitude, Radius
Time: 09, 00, 00, 28800000
Cancel Save

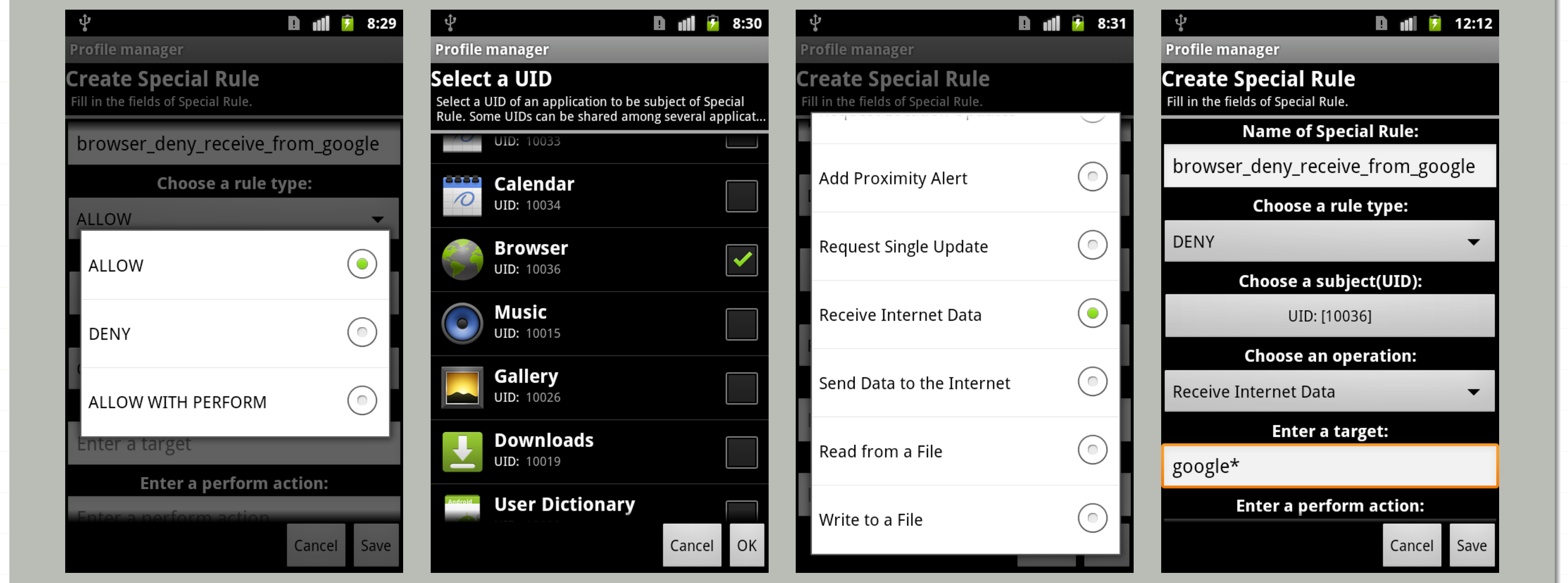
(b) Context configuration

Figure 3: Security Profile change

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



8:29
Profile manager
Create Special Rule
Fill in the fields of Special Rule.
browser_deny_receive_from_google
Choose a rule type: ALLOW
○ ALLOW ●
DENY ○
ALLOW WITH PERFORM ○
Enter a target
Enter a perform action:
Cancel Save

(a) Rule type selection

8:30
Profile manager
Select a UID
Select a UID of an application to be subject of Special Rule. Some UIDs can be shared among several applicat...
UID: 10033 □
Calendar UID: 10034 □
Browser UID: 10036 ☑
Music UID: 10015 □
Gallery UID: 10026 □
Downloads UID: 10019 □
User Dictionary □
Cancel OK

(b) Subject of the Special Rule

8:31
Profile manager
Create Special Rule
Fill in the fields of Special Rule.
Add Proximity Alert ○
Request Single Update ○
Receive Internet Data ●
Send Data to the Internet ○
Read from a File ○
Write to a File ○

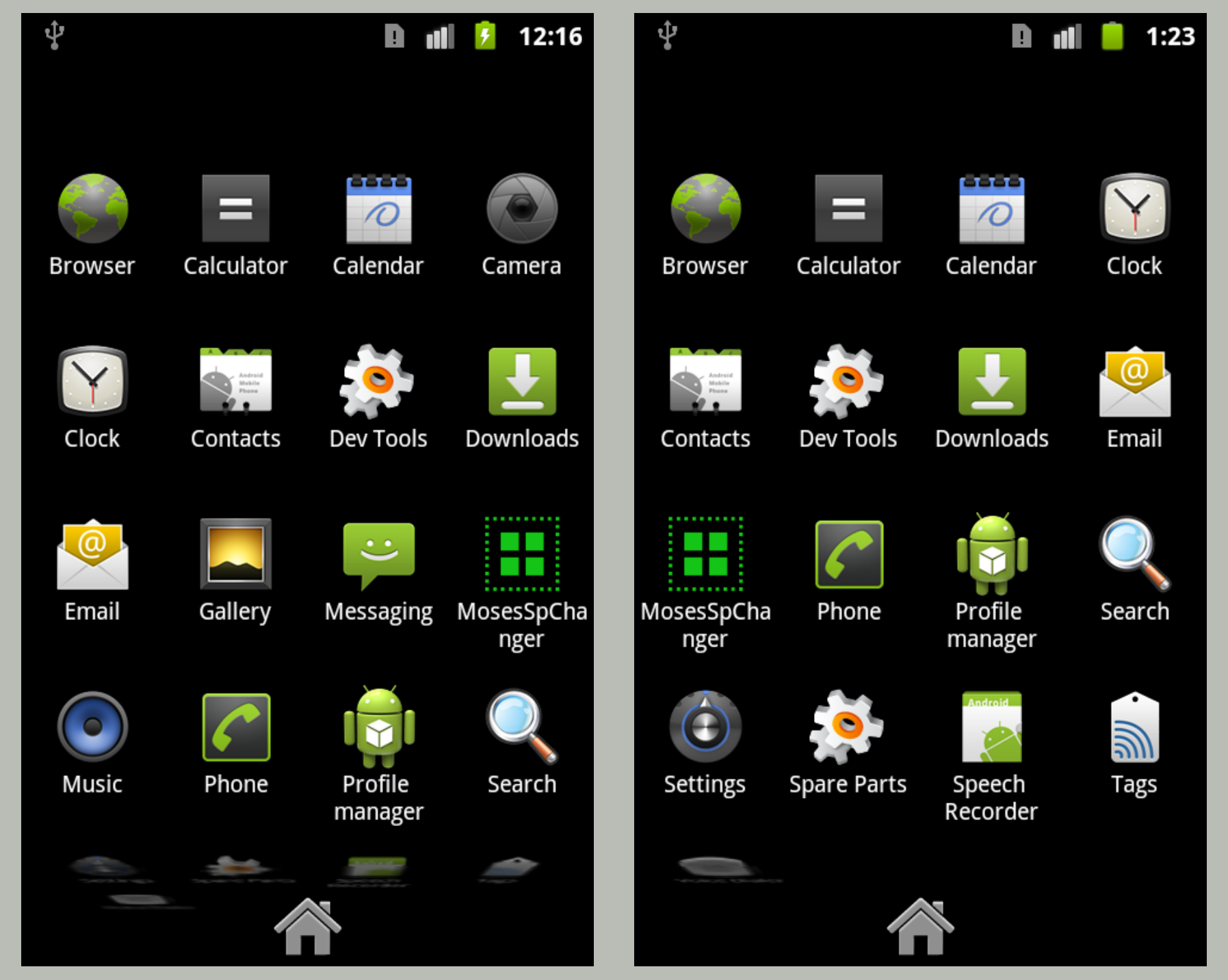
(c) Operation selection

12:12
Profile manager
Create Special Rule
Fill in the fields of Special Rule.
Name of Special Rule: browser_deny_receive_from_google
Choose a rule type: DENY
Choose a subject(UID): UID: [10036]
Choose an operation: Receive Internet Data
Enter a target: google*
Enter a perform action:
Cancel Save

(d) Final view of the Special Rule

Figure 4: Configuration of Moses Special Rule

MOSES operation



(a) All applications allowed (SP: private)

(b) Camera, Gallery, Messaging, Music applications not allowed (SP: work)

Figure 5: Main window of Launcher application

19th ACM Conference on Computer and Communications Security (CCS 2012), Raleigh, NC, USA, October 16–18, 2012.