

A certified reference validation mechanism for the permission model of Android ^{*}

Gustavo Betarte¹, Juan Campo¹, Felipe Gorostiaga², and Carlos Luna¹

¹ InCo, Facultad de Ingeniería, Universidad de la República, Uruguay.

{gustun,jdcampo,cluna}@fing.edu.uy

² IMDEA Software Institute, Spain.

felipe.gorostiaga@imdea.org

Abstract. Android embodies security mechanisms at both OS and application level. In this platform application security is built primarily upon a system of permissions which specify restrictions on the operations a particular process can perform. The critical role of these security mechanisms makes them a prime target for (formal) verification. We present an idealized model of a reference monitor of the novel mechanisms of Android 6 (and further), where it is possible to grant permissions at run time. Using the programming language of the proof-assistant `Coq` we have developed a functional implementation of the reference validation mechanism and certified its correctness with respect to the specified reference monitor. Several properties concerning the permission model of Android 6 and its security mechanisms have been formally formulated and proved. Applying the program extraction mechanism provided by `Coq` we have also derived a certified `Haskell` prototype of the reference validation mechanism.

1 Introduction

The Android [19] platform for mobile devices captures more than 85% of the total market-share [14]. Mobile devices allow people to develop multiple tasks in different areas, regrettably, the benefits of using them are counteracted by increasing security risks.

Android embodies security mechanisms at both OS and application level. Application security is built primarily upon a system of permissions, which specify restrictions on the operations a particular process can perform. Permissions in Android are basically tags that developers declare in their applications, more precisely in the so-called application *manifest*, to gain access to sensitive resources. On all versions of Android an application must declare both the normal and the dangerous permissions it needs in its application manifest. However, the effect of that declaration is different depending on the system version and the application's target SDK level [3]. In particular, if a device is running Android 6

^{*} Partially funded by project ANII-FCE_1_2014_1_103803: Mecanismos autónomos de seguridad certificados para sistemas computacionales móviles, Uruguay.

(Marshmallow) and the application’s target SDK is 23 or higher the application has to list the permissions in the manifest, and it must request each dangerous permission it needs while the application is running. The user can grant or deny each permission, and the application can continue to run with limited capabilities even if the user denies a permission request. This modification of the access control and decision process, on the one side, streamlines the application install process, since the user does not need to grant permissions when he/she installs or updates an application. On the other hand, as users can revoke the (previously granted) permissions at any time, the application needs to check whether it has the corresponding privileges every time it attempts to access a resource on the device [3]. The important and critical role of these security mechanisms makes them a prime target for (formal) verification.

Security models play an important role in the design and evaluation of security mechanisms of systems. Their importance was already pointed out in 1972 in the Anderson report [1], where the concept of *reference monitor* was first introduced. This concept defines the design requirements for implementing what is called a *reference validation mechanism*, which shall be responsible for enforcing the access control policy of a system. The work presented here is concerned with the formal analysis and verification of properties performed on an idealized model that abstracts away the specifics of any particular implementation, and yet provides a realistic setting in which to explore the issues that pertain to the realm of (critical) security mechanisms of Android.

Contributions In [8,9], we have presented a formal specification of an idealized formulation of the permission model of version 5 of Android. Here we present an enriched version of that model which can be used to perform a formal analysis of the novel mechanisms of Android 6, which make it possible to grant permissions at run time. Furthermore, using the programming language of **Coq** [22] we have developed an executable (functional) specification of the reference validation mechanism and it has been proved that those functions conform to the axiomatic specification as specified in the model. Additionally, and using the program extraction mechanism provided by **Coq**, we have derived a certified **Haskell** prototype of the reference validation mechanism. Several properties concerning the security model of Android 6 have been formally formulated and proved.

Organization of the paper Section 2 reviews the security mechanisms of Android. Section 3 describes the formal axiomatic specification of the Android security system and discusses some of the verified properties. Section 4 presents a functional (operational) semantics of the specified reference monitor and outlines its proof of correctness. This section also discusses security properties satisfied by the certified implementation of the security mechanisms. Section 5 considers related work and finally, Section 6 concludes with a summary of our contributions and directions for future work. The full formalization may be obtained from [15] and verified using the **Coq** proof assistant.

2 Android's security model

The architecture of Android takes the form of a software stack which comprises an OS, a run-time environment, middleware, services and libraries, and applications. An Android application is built up from *components*. A component is a basic unit that provides a particular functionality and that can be run by any other application with the right permissions. There exist four types of components [2]: i) *activity*, which is essentially a user interface of the application; ii) *service*, a component that executes in background without providing an interface to the user; iii) *content provider*, a component intended to share information among applications; and iv) *broadcast receiver*, a component whose objective is to receive messages, sent either by the system or an application, and trigger the corresponding actions. Activities, services and broadcast receivers are activated by a special kind of message called *intent*. An intent makes it possible for different components to interact at runtime. A intent filter specifies the types of intents that a component receiver can respond to [2]. Applications usually need to use system resources to execute properly. Since applications run inside sandboxes, this entails the existence of a decision procedure (a reference validation mechanism) that guarantees the authorized access to those resources. Decisions are made by following security policies using a simple notion of permission. Every permission is identified by a name/text, has a protection level and may belong to a permission group. There exist two principal classes of permissions: the ones defined by the application, for the sake of self-protection; and those predefined by Android, which are intended to protect access to resources and services of the system. An application declares –in a XML file called **AndroidManifest**– the set of permissions it needs to acquire further capacities than the default ones. When an action involving permissions is required, the system determines which permissions every application has and either allows or denies its execution.

Depending on the protection level of the permission, the system defines the corresponding decision procedure [4]. There are four classes of permission levels: i) *Normal*, assigned to low risk permissions that grant access to isolated characteristics; ii) *Dangerous*, permissions of this level are those that provide access to private data or control over the device. From version 6 of Android dangerous permissions are not granted at installation time; iii) *Signature*, a permission of this level is granted only if the application that requires it and the application that defined it are both signed with the same certificate; and iv) *Signature/System*, this level is assigned to permissions that regulate the access to critical system resources or services. Additionally, an application can also declare the permissions that are needed to access it. A running application may ask the user to grant it dangerous permission groups and ungrouped permissions, who in turn can accept or decline this request.

If the execution of an action requires for an application to have certain permission the system will first make sure that this holds by means of the following rules: i) the application must declare the permission as used in its manifest; ii) if the permission is of level *Normal*, then the application does have it; iii) if the permission is of level *Dangerous* and belongs to a permission group, such group

must have been granted to the application; iv) if the permission is of level *Dangerous* but is ungrouped, then it must have been individually granted to the application; v) if the permission is of level *Signature*, then the both the involved application and the one that declares it must have been signed with the same certificate; vi) lastly, if the permission is of level *Signature/System*, then the involved application must have been signed with either the same certificate as the one who declares it or the certificate of the device manufacturer. Otherwise, an error is thrown and the action is not executed.

Android provides two mechanisms by which an application can delegate its own permissions to another one. These mechanisms are called *pending intents* and *URI permissions*. An intent may be defined by a developer to perform a particular action. A `PendingIntent` is an object which is associated to the action, a reference that might be used by another application to execute that action. The *URI permissions* mechanism can be used by an application that has read/write access to a *content provider* to delegate those permissions to another application.

3 Formalization of the permission model

In this section we provide a short account of the axiomatic semantics of the Android security system and discuss some of the verified security properties.

Formal language used The `Coq` proof assistant provides a (dependently typed) functional programming language and a reasoning framework based on higher order logic to perform proofs of (complex) specifications and programs. `Coq` allows developing mathematical facts. This includes defining objects (sets, lists, streams, functions, programs); making statements (using basic predicates, logical connectives and quantifiers); and finally writing proofs. The type of propositions is called `Prop`. The `Coq` environment provides program extraction towards languages like Ocaml and Haskell for execution of (certified) algorithms [16,17].

In this work, enumerated types and sum types are defined using Haskell-like notation; for example, $\text{option } T \stackrel{\text{def}}{=} \text{None} \mid \text{Some } (t : T)$. Record types are of the form $\{l_1 : T_1, \dots, l_n : T_n\}$, whereas their elements are of the form $\{t_1, \dots, t_n\}$. Field selection is written as $r.l_i$. We also use $\{T\}$ to denote the set of elements of type T . Finally, the symbol \times defines tuples, and *nat* is the datatype of natural numbers. We omit `Coq` code for reasons of clarity; this code is available in [15].

3.1 Model states

The Android security model we have developed has been formalized as an abstract state machine. In this model, states (`AndroidST`) are modelled as 12-tuples that respectively store data about the applications installed, their permissions and the running instances of components; the formal definition appears in Figure 1.

The type `PermId` represents the set of permissions identifiers; `PermGroup`, the set of permission groups identifiers; `Comp`, the application components whose

OpTy	::= <i>read</i> <i>write</i> <i>rw</i>
PermLvl	::= <i>dangerous</i> <i>normal</i> <i>signature</i> <i>Signature/System</i>
Perm	::= PermId \times <i>option</i> PermGroup \times PermLvl
InstApps	::= {AppId}
PermsGr	::= {AppId \times PermGroup}
AppPS	::= {AppId \times PermId}
CompInstance	::= iComp \times Comp
CompInsRun	::= {CompInstance}
DelPPerms	::= {AppId \times ContProv \times Uri \times OpTy}
DelTPerms	::= {iComp \times ContProv \times Uri \times OpTy}
ARVS	::= {AppId \times Res \times Val}
Intents	::= {iComp \times Intent}
Manifest	::= {Comp} \times <i>option nat</i> \times <i>option nat</i> \times {PermId} \times {Perm} \times <i>option</i> PermId
Manifests	::= {AppId \times Manifest}
Certs	::= {AppId \times Cert}
AppDefPS	::= {AppId \times Perm}
SysImage	::= {SysImgApp}
AndroidST	::= InstApps \times PermsGr \times AppPS \times CompInsRun \times DelPPerms \times DelTPerms \times ARVS \times Intents \times Manifests \times Certs \times AppDefPS \times SysImage

Fig. 1. Android state

code will run on the system; **AppId** represents the set of application identifiers; **iComp** is the set of identifiers of running instances of application components; **ContProv** is a subset of **Comp**, a special type of component that allows sharing resources among different applications; a member of the type **Uri** is a particular uri (uniform resources identifier); the type **Res** represents the set of resources an application can have (through its *content providers*, members of **ContProv**); the type **Val** is the set of possible values that can be written on resources; an intent –i.e. a member of type **Intent**– represents the intention of a running component instance to start or communicate with other applications; a member of **SysImgApp** is a special kind of applications which are deployed along with the OS itself and has certain privileges, like being impossible to uninstall.

The first component of a state records the identifiers (**AppId**) of the applications installed by the user. The second and third components of the state keep track, respectively, of the permission groups (**PermGroup**) and ungrouped permissions granted to each application present in the system, both the ones installed by the user and the system applications. The fourth component of the state stores the set of running component instances (**CompInstance**), while the components **DelPPerms** and **DelTPerms** store the information concerning permanent and temporary permissions delegations, respectively³. The seventh and eighth components of the state store respectively the values (**Val**) of resources (**Res**) of applications and the set of intents (**Intent**) sent by running instances of components (**iComp**) not yet processed. The four last components of the state record information that represents the manifests of the applications installed by the user, the certificates (**Cert**) with which they were signed and the set of per-

³ A permanent delegated permission represents that an app has delegated permission to perform an operation on the resource identified by an URI. A temporary delegated permission refers to a permission that has been delegated to a component instance.

missions they define. The last component of the state stores the set of (native) applications installed in the Android system image, information that is relevant when granting permissions of level *Signature/System*. A manifest (**Manifest**) is modelled as a 6-tuple that respectively declare application components (set of components, of type **Comp**, included in the application); optionally, the minimum version of the Android SDK required to run the application; optionally, the version of the Android SDK targeted on development; the set of permissions it may need to run at its maximum capability; the set of permissions it declares; and the permission required to interact with its components, if any. Application components are all denoted by a component identifier. A content provider (**ContProv**), in addition, encompasses a mapping to the managed resources from the URIs assigned to them for external access. While the components constitute the static building blocks of an application, all runtime operations are initiated by component instances, which are represented in our model as members of an abstract type.

We define a notion of valid state, through the predicate *valid_state* on the elements of type **AndroidST**, that captures several well-formedness conditions. The definition is provided in Appendix A.

3.2 Action semantics

The axiomatic semantics of the Android security system is modeled by defining a set of actions, and providing their semantics as state transformers. Table 1 summarises a subset of the actions specified in our model, which provide coverage to the different functionalities of the Android security model.

The behaviour of actions (of type **Action**) is specified by a precondition *Pre* and by a postcondition *Post* of respective types: $Pre : \mathbf{AndroidST} \rightarrow \mathbf{Action} \rightarrow Prop$, and $Post : \mathbf{AndroidST} \rightarrow \mathbf{Action} \rightarrow \mathbf{AndroidST} \rightarrow Prop$. For instance, the axiomatic semantics of the **install** action is given by:

$$\begin{aligned}
 Pre(s, \mathbf{install} \ app \ m \ c \ lRes) &\stackrel{\text{def}}{=} \\
 &\neg isAppInstalled(app, s) \wedge \neg has_duplicates_cmp(m) \wedge \\
 &\forall c : \mathbf{Comp}, c \in cmp(m) \rightarrow c \notin cmpInState(s) \wedge \\
 &\neg hasDuplicates_perm(m) \wedge authPerms(m, s) \wedge \\
 &\forall c : \mathbf{Comp}, c \in cmp(m) \rightarrow cmpDeclareIntentFilterCorrectly(c) \\
 Post(s, \mathbf{install} \ app \ m \ c \ lRes, s') &\stackrel{\text{def}}{=} \\
 &addManifest(m, app, s, s') \wedge addCert(c, app, s, s') \wedge \\
 &addDefPerms(app, m, s, s') \wedge addApp(app, s, s') \wedge \\
 &addRes(app, lRes, s, s') \wedge initializePermLists(app, s, s') \wedge \\
 &sameOtherFields_install(s, s')
 \end{aligned}$$

The precondition of action **install** $app \ m \ c \ lRes$ in a state s requires that the application is not already installed, and that no system application has its same identifier ($\neg isAppInstalled(app, s)$). The identifiers of the components listed in its manifest ($c \in cmp(m)$) must be different from each other ($\neg has_duplicates_cmp(m)$), and also different from those of the components already present in the device ($c \notin cmpInState(s)$). The permissions defined by the application to be

install <i>app m c lRes</i>	Install application with id <i>app</i> , whose manifest is <i>m</i> , is signed with certificate <i>c</i> and its resources list is <i>lRes</i> .
uninstall <i>app</i>	Uninstall the application with id <i>app</i> .
grant <i>p app</i>	Grant the permission <i>p</i> to the application <i>app</i> .
revoke <i>p app</i>	Remove the permission <i>p</i> from the application <i>app</i> .
grantPermGroup <i>g app</i>	Grant the permission group <i>g</i> to the application <i>app</i> .
revokePermGroup <i>g app</i>	Remove the permission group <i>g</i> from the application <i>app</i> .
hasPermission <i>p app</i>	Check if the application <i>app</i> has the permission <i>p</i> .
read <i>ic cp u</i>	The running comp. <i>ic</i> reads the resource corresponding to URI <i>u</i> from content provider <i>cp</i> .
write <i>ic cp u val</i>	The running comp. <i>ic</i> writes value <i>val</i> on the resource corresponding to URI <i>u</i> from content provider <i>cp</i> .
startActivity <i>i ic</i>	The running comp. <i>ic</i> asks to start an activity specified by the intent <i>i</i> .
startActivityRes <i>i n ic</i>	The running comp. <i>ic</i> asks to start an activity specified by the intent <i>i</i> , and expects as return a token <i>n</i> .
startService <i>i ic</i>	The running comp. <i>ic</i> asks to start a service specified by the intent <i>i</i> .
sendBroadcast <i>i ic p</i>	The running comp. <i>ic</i> sends the intent <i>i</i> as broadcast, specifying that only those components who have the permission <i>p</i> can receive it.
sendOrdBroadcast <i>i ic p</i>	The running comp. <i>ic</i> sends the intent <i>i</i> as an ordered broadcast, specifying that only those components who have the permission <i>p</i> can receive it.
sendSBroadcast <i>i ic</i>	The running comp. <i>ic</i> sends the intent <i>i</i> as a sticky broadcast.
resolveIntent <i>i app</i>	Application <i>app</i> makes the intent <i>i</i> explicit.
receiveIntent <i>i ic app</i>	Application <i>app</i> receives the intent <i>i</i> , sent by the running comp. <i>ic</i> .
stop <i>ic</i>	The running comp. <i>ic</i> finishes its execution.
grantP <i>ic cp app u pt</i>	The running comp. <i>ic</i> delegates permanent permissions to application <i>app</i> . This delegation enables <i>app</i> to perform operation <i>pt</i> on the resource assigned to URI <i>u</i> from content provider <i>cp</i> .
revokeDel <i>ic cp u pt</i>	The running comp. <i>ic</i> revokes delegated permissions on URI <i>u</i> from content provider <i>cp</i> to perform operation <i>pt</i> .
call <i>ic sac</i>	The running comp. <i>ic</i> makes the API call <i>sac</i> .

Table 1. Actions

installed must be different from each other ($\neg hasDuplicates_perm(m)$) as well as different from those defined by other applications ($authPerms(m, s)$). Finally, the intent filters of its components ($c \in cmp(m)$) must be well defined; the specified types of intents must match ($cmpDeclareIntentFilterCorrectly(c)$).

The postcondition of action **install** *app m c lRes*, with initial state *s* and final state *s'*, specifies that its manifest (*m*), the certificate with which it was signed (*c*) and the permissions it defines that are not system permissions must be added to the state bound to the application identifier (predicates *addManifest*, *addCert*, and *addDefPerms*); which in turn must be included in the list of installed applications (*addApp(app, s, s')*). The application resources are initialized with the initial value *initVal* (*addRes(app, lRes, s, s')*), while the lists of permission and permission groups granted to the application are initialized as empty (*initializePermLists(app, s, s')*). The rest of the system components remain unchanged (*sameOtherFields_install(s, s')*).

3.3 Executions

There can be attempts to execute an action on a state that does not verify the precondition of that action. In the presence of one such situation the system answers with a corresponding error code (of type *ErrorCode*).

Executing an action a over a valid state s produces a new state s' and a corresponding answer r (denoted $s \xrightarrow{a/r} s'$), where the relation between the former state and the new one is given by the postcondition relation $Post$.

$$\frac{valid_state(s) \quad Pre(s, a) \quad Post(s, a, s')}{s \xrightarrow{a/ok} s'} \quad \frac{valid_state(s) \quad ErrorMessage(s, a, ec)}{s \xrightarrow{a/error(ec)} s}$$

Whenever an action occurs for which the precondition holds, the valid state may change in such a way that the action postcondition is established. The notation $s \xrightarrow{a/ok} s'$ may be read as *the execution of the action a in a valid state s results in a new state s'* . However, if the precondition is not satisfied, then the valid state s remains unchanged and the system answer is the error message determined by a relation $ErrorMessage$ ⁴. Formally, the possible answers of the system are defined by the type $Response \stackrel{\text{def}}{=} ok \mid error \ (ec : ErrorCode)$, where ok is the answer resulting from a successful execution of an action. One-step execution with error management preserves valid states.

Lemma 1 (Validity is invariant).

$$\forall (s \ s' : \text{AndroidST})(a : \text{Action})(r : \text{Response}), s \xrightarrow{a/r} s' \rightarrow valid_state(s')$$

The results presented in this work are obtained from valid states of the system.

3.4 Reasoning over the specified reference monitor

In this section we present and discuss some relevant properties that can be established concerning the Android Marshmallow security framework. In particular we shall focus on vulnerabilities that if exploited would allow violations to the intended security policy. The helper functions and predicates used to define the properties and lemmas discussed in this paper are presented and described in Table 2. The full formal definition of the lemmas as well as those of other security properties that were formally analyzed can be found in [15], along with their corresponding proofs. We also include an informal description of each property, in italics. The first property presents a controversial characteristic of Android's new permission system. For example, as the dangerous permissions `READ_CONTACTS` (required for reading the contact list) and `WRITE_CONTACTS` (required for writing the contact list) both belong to the permission group `CONTACTS`, none of them can be individually granted. Instead, the application must be granted the permission group `CONTACTS`, giving it the right to both reading and writing the user's contact list. This violates the intended least privilege security policy claimed by the designers of the platform.

Property 1 (No fine control over grouped permissions)

$$\forall (s, s' : \text{AndroidST})(p : \text{Perm})(g : \text{PermGroup})(app : \text{AppId}), \\ permissionIsGrouped(p) \rightarrow \neg s \xrightarrow{grant \ p \ app/ok} s'$$

⁴ Given a state s , an action a and an error code ec , $ErrorMessage(s, a, ec)$ holds iff $error \ ec$ is an acceptable response when the execution of a is requested on state s .

Function/Predicate	Description
$appHasPermission(app, p, s)$	holds iff app is considered to have permission p on state s .
$canGrant(cp, u, s)$	holds iff the content provider cp allows the delegation of permissions over the resource at URI u on state s .
$canStart(c', c, s)$	holds if the app containing component c' (installed in s) has the required permissions to create a new running instance of c .
$cmpProtectedByPerm(c)$	returns the permission by which the component c is protected.
$componentIsExported(c)$	holds iff the component c is exported and can be accessed from other applications.
$existsRes(cp, u, s)$	holds iff the URI u belongs to the content provider cp on s .
$getAppFromCmp(c, s)$	given a component c on s , returns the app to which it belongs.
$getAppRequestedPerms(m)$	given the manifest m of an app, returns the set of permissions it uses.
$getDefPermsForApp(app, s)$	returns the set of permissions defined by app on state s .
$getGrantedPermsForApp(app, s)$	returns the set of individual permissions granted to app on s .
$getInstalledApps(s)$	returns the set of identifiers of the applications installed on s .
$getManifestForApp(app, s)$	returns the manifest of application app on state s .
$getPermissionId(p)$	returns the identifier of permission p .
$getPermissionLevel(p)$	returns the permission level of permission p .
$getRunningComponents(s)$	returns the set of pairs consisting of a running instance id, and its associated component currently running on state s .
$inApp(c, app, s)$	holds iff the component c belongs to application app on state s .
$permissionIsGrouped(p)$	holds iff permission p belongs to any permission group.
$permissionRequiredForRead(c)$	returns the permission required for reading the component.
$permSACs(p, sac)$	holds iff permission p is required for performing the system call sac (of type $SACall$).

Table 2. Helper functions and predicates

Android's permission system is not granular enough for granting a proper subset of the set of permissions that belong to a group.

The next property formalizes another weak point in the specification of Android's new permission system: in a valid state an application may have the right of writing the contact list (WRITE_CONTACTS) even if this permission was never individually granted.

Property 2 (Implicit individual permission granting)

$$\begin{aligned} &\exists(s : \text{AndroidST})(p : \text{Perm})(app : \text{AppId}), \text{valid_state}(s) \wedge \\ &\text{getPermissionLevel}(p) = \text{dangerous} \wedge p \notin \text{getGrantedPermsForApp}(app, s) \wedge \\ &p \notin \text{getDefPermsForApp}(app, s) \wedge appHasPermission(app, p, s) \end{aligned}$$

Applications may obtain privileges that were never granted to it.

In Android 6 an application that wishes to send information through the network must have the permission INTERNET but, since this permission is of level *normal*, any application that lists it as used in its manifest file has the right to access the network in an implicit and irrevocable way. Once again, this has been criticized due to the potential information leakage it allows. The following property formally generalizes this situation and embodies a reasonable argument to roll back this security issue introduced in Android Marshmallow.

Property 3 (Internet access implicitly and irrevocably allowed)

$$\forall(s : \text{AndroidST})(sac : \text{SACall})(c : \text{Comp})(ic : \text{iComp})(p : \text{Perm}),$$

$$\begin{aligned}
& \text{valid_state}(s) \rightarrow \text{permSAC}(p, \text{sac}) \rightarrow \\
& \text{getPermissionLevel}(p) = \text{normal} \rightarrow \text{getPermissionId}(p) \in \\
& \text{getAppRequestedPerms}(\text{getManifestForApp}(\text{getAppFromCmp}(c, s), s)) \rightarrow \\
& (ic, c) \in \text{getRunningComponents}(s) \rightarrow s \xrightarrow{\text{call } ic \text{ sac}/ok} s
\end{aligned}$$

If the execution of an Android API call only requires permissions of level normal, it is enough for an application to list them as used on its manifest file to be allowed to perform such call.

4 A certified reference validation mechanism

The implementation of the Android security system that we have developed consists of a set of **Coq** functions such that for every predicate involved in the axiomatic specification of action execution there exists a function which stands for the functional counterpart of that predicate. In this section we show how the correctness of the implementation is certified by a formal proof that establishes its soundness with respect to the inductive (axiomatic) semantics of the Android security mechanisms. The execution of an action has been implemented as a *step* function that given a system state s and an action a invokes the function that implements the execution of a in s and returns an object res of type $Result \stackrel{\text{def}}{=} \{resp : Response, st : \text{AndroidST}\}$, where $res.resp$ is either an error code ec , if the precondition of the actions does not hold in state s , or otherwise the value ok , and the state $res.st$ represents the execution effect. The *step* function acts basically as an action dispatcher. Figure 2, which shows the structure of the dispatcher, details the branch corresponding to the dispatching of action **install**, which is the action we shall use along this section to illustrate the working of the implementation. The functions invoked in the branches, like

```

Definition step( $s, a$ ) :=
  match  $a$  with
    | ...  $\Rightarrow$  ...
    | install  $app\ m\ c\ lRes \Rightarrow install\_safe(app, m, c, lRes, s)$ 
    | ...  $\Rightarrow$  ...
  end.

Definition install\_safe( $app, m, c, lRes, s$ ) : Result :=
  match install\_pre( $app, m, c, lRes, s$ ) with
    | Some  $ec \Rightarrow \{error(ec), s\}$ 
    | None  $\Rightarrow \{ok, install\_post(app, m, c, lRes, s)\}$ 
  end.

```

Fig. 2. The *step* function and execution of **install** action

install_safe, are state transformers whose definition follows this pattern: first it is checked whether the precondition of the action is satisfied in state s , and then, if that is the case, the function that implements the execution of the action is invoked. Otherwise, the state s , unchanged, is returned along with an appropriate response specifying an error code which describes the failure. In this figure we

also describe the function that implements the execution of the `install` action. The `Coq` code of this function, together with that of the remaining functions, can be found in [15]⁵. The function `install_pre` is defined as the nested validation of each of the properties of the precondition, specifying which error to throw when one of them doesn't hold. The function `install_post` implements the expected behavior of the `install` action: the identifier of the application is prepended to the list of installed applications, both the list of granted permission and the list of granted permission groups are initialized as empty for it, its resource list is added to the system, and its manifest, certificate and defined permissions are included in the system state⁶.

4.1 Soundness

We proceed now to outline the proof that the functional implementation of the security mechanisms of Android correctly implements the axiomatic model. This correctness property has been formally stated as a soundness theorem and verified using `Coq` [15].

Theorem 1 (Soundness of Android security system implementation).

$$\forall (s : \text{AndroidST}) (a : \text{Action}), \text{valid_state}(s) \rightarrow s \xrightarrow{a/\text{step}(s,a).resp} \text{step}(s,a).st$$

The proof of this theorem follows by, in the first place, performing a case analysis on $\text{Pre}(s,a)$ (this predicate is decidable) and then in the case that $\text{Pre}(s,a)$ applying Lemma 2; otherwise applying Lemma 4.

Lemma 2 (Soundness of valid execution).

$$\begin{aligned} \forall (s : \text{AndroidST}) (a : \text{Action}), \text{valid_state}(s) \rightarrow \text{Pre}(s,a) \rightarrow \\ s \xrightarrow{a/ok} \text{step}(s,a).st \wedge \text{step}(s,a).resp = ok \end{aligned}$$

The proof of Lemma 2 proceeds by applying functional induction on $\text{step}(s,a)$ and then by providing the corresponding proof of soundness of the function that implements the execution of each action. Thus, in the case of the action `install` we have stated and proved Lemma 3. This lemma, in turn, follows by performing a case analysis on the result of applying the function `install_pre` on s and the action: if the result is an error code then the thesis follows by contradiction. Otherwise, it follows by the correctness of the function `install_post`.

Lemma 3 (Correctness of install execution).

$$\begin{aligned} \forall (s : \text{AndroidST}) (app : \text{App}) (m : \text{Manifest}) (c : \text{Cert}) (lRes : \text{list Res}), \\ \text{valid_state}(s) \rightarrow \text{Pre}(s, \text{install } app \ m \ c \ lRes) \rightarrow \\ \text{Post}(s, \text{install } app \ m \ c \ lRes, \text{install_post}(app, m, c, lRes, s)) \end{aligned}$$

As to Lemma 4, the proof also proceeds by first applying functional induction on $\text{step}(s,a)$. Then, for each action a , it is shown that if $\neg \text{Pre}(s,a)$ the execution of the function that implements that action yields the values returned by the branch corresponding to the case that the function that validates the precondition of the action a in state s fails, i.e., an error code ec and the (unchanged) state s .

⁵ We omit here the formal definition of these functions due to space constraints.

⁶ We implement the sets in the model with lists of `Coq`.

Lemma 4 (Soundness of error execution).

$$\forall (s : \text{AndroidST}) (a : \text{Action}), \text{valid_state}(s) \rightarrow \neg \text{Pre}(s, a) \rightarrow \exists (ec : \text{ErrorCode}), \\ \text{step}(s, a).st = s \wedge \text{step}(s, a).resp = \text{error}(ec) \wedge \text{ErrorMsg}(s, a, ec)$$
4.2 Reasoning over the certified reference validation mechanism

We have modeled the execution of the permission validation mechanism during a session of the system as a function that implements the execution of a list of actions starting in an (initial) system state. The output of the execution, a trace, is the corresponding sequence of states.

Function *trace* (*s* : *AndroidST*) (*actions* : *list Action*) : *list AndroidST* :=
match *actions* **with**
| *nil* \Rightarrow *nil*
| *action* :: *rest* \Rightarrow **let** *s'* := (*step s action*).*st* **in** *s'* :: *trace s' rest*
end.

We have stated and proved several security properties over the function *trace*. In what follows *s*, *initstate*, *sndstate* and *laststate* stand for variables of type *AndroidST*, *p* is a variable of type *Perm*, *app* and *app'* of type *AppId* and *l* of type *list Action*. We present first a property that formally states that in version 6 of the OS for an application to have a non-grouped dangerous permission it must be explicitly granted to it.

Property 4 (Dangerous permissions must be explicitly granted)

$$\begin{aligned} &\text{valid_state}(\text{initState}) \rightarrow \text{app} \in \text{getInstalledApps}(\text{initState}) \rightarrow \\ &\text{getPermissionLevel}(p) = \text{dangerous} \rightarrow \text{permissionIsGrouped}(p) = \text{None} \rightarrow \\ &\text{appHasPermission}(\text{app}, p, \text{lastState}) \rightarrow \\ &\neg \text{appHasPermission}(\text{app}, p, \text{initState}) \rightarrow \text{uninstall app} \notin l \rightarrow \\ &\text{last}(\text{trace}(\text{initState}, l), \text{initState}) = \text{lastState} \rightarrow \text{grant } p \text{ app} \in l \end{aligned}$$

A non-grouped dangerous permission can only be explicitly granted to an application.

With the following property we formally state, and prove, that if an application used to have a permission that was later revoked, only re-granting it will allow the application to have it again.

Property 5 (Revoked permissions must be regranted)

$$\begin{aligned} &\text{valid_state}(\text{initState}) \rightarrow \text{getPermissionLevel}(p) = \text{dangerous} \rightarrow \\ &\text{permissionIsGrouped}(p) = \text{None} \rightarrow p \notin \text{getDefPermsForApp}(\text{app}, \text{initState}) \rightarrow \\ &\text{step}(\text{initState}, \text{revoke } p \text{ app}).st = \text{sndState} \rightarrow \\ &\text{step}(\text{initState}, \text{revoke } p \text{ app}).resp = \text{ok} \rightarrow \text{uninstall app} \notin l \rightarrow \text{grant } p \text{ app} \notin l \rightarrow \\ &\text{last}(\text{trace}(\text{sndState}, l), \text{sndState}) = \text{lastState} \rightarrow \\ &\neg \text{appHasPermission}(\text{app}, p, \text{lastState}) \end{aligned}$$

If an application used to have a permission that was later revoked, only regranted it will allow the application to have it again.

Certain assertions on which a developer could rely in previous versions of Android OS do not hold in its latest version. The following property states that a running component may have the right of starting another one on a certain state, but may not be able to do so at a later time.

Property 6 (The right to start an external component is revocable)

$$\begin{aligned}
& \forall (c : \text{Comp})(act : \text{Activity}) \text{ valid_state}(initState) \rightarrow \\
& \text{getPermissionLevel}(p) = \text{dangerous} \rightarrow \text{permissionIsGrouped}(p) = \text{None} \rightarrow \\
& app \neq app' \rightarrow p \notin \text{getDefPermsForApp}(app, initState) \rightarrow \text{inApp}(c, app, initState) \rightarrow \\
& \text{inApp}(act, app', initState) \rightarrow \text{cmpProtectedByPerm}(act) = \text{Some } p \rightarrow \\
& \text{canStart}(c, act, initState) \rightarrow \exists (l : \text{list Action}), \text{uninstall } app \notin l \wedge \\
& \text{uninstall } app' \notin l \wedge \neg \text{canStart}(c, act, \text{last}(\text{trace}(initState, l), initState))
\end{aligned}$$

A running component may have the right of starting another one on a certain state, but may not be able to do so at a later time.

When an application app is granted a permission p to access certain resource, it is also given the right to delegate this ability to another application, say app' , to access that same resource on its behalf. However, if p is revoked from the application app , the permission delegations is not invalidated and thus the application app' may still be able to access the resource. This property is a proof that the current specification allows a behavior which is arguably against the user's will.

Property 7 (Delegated permissions are not recursively revoked)

$$\begin{aligned}
& \forall (ic, ic' : \text{iComp})(c, c' : \text{Comp})(u : \text{uri})(cp : \text{CProvider}), \\
& \text{valid_state}(s) \rightarrow \text{step}(s, \text{grant } p \text{ app}).\text{resp} = \text{ok} \rightarrow \\
& \text{getAppFromCmp}(c, s) = \text{app} \rightarrow \text{getAppFromCmp}(c', s) = \text{app}' \rightarrow \\
& (ic, c) \in \text{getRunningComponents}(s) \rightarrow (ic', c') \in \text{getRunningComponents}(s) \rightarrow \\
& \text{canGrant}(cp, u, s) \rightarrow \text{existsRes}(cp, u, s) \rightarrow \text{componentIsExported}(cp) \rightarrow \\
& \text{permissionRequiredForRead}(cp) = \text{Some } p \rightarrow \\
& \text{let opsResult} := \text{trace}(s, [\text{grant } p \text{ app}, \text{grantP } ic \text{ cp app}' u \text{ Read}, \\
& \text{revoke } p \text{ app}]) \text{ in } \text{step}(\text{last}(\text{opsResult}, s), \text{read } ic' \text{ cp } u).\text{resp} = \text{ok}
\end{aligned}$$

In Android 6 if a permission p is revoked for an application app not necessarily shall be revoked for the applications to which app delegated p .

5 Related work

Several analyses have been carried out concerning the security of the Android system [11, 18, 10, 12, 13]. Few works, however, pay attention to the formal aspects of the permission enforcing framework. In particular, Shin *et al.* [20, 21] build a formal framework that represents the Android permission system, which is developed in Coq, as we do. However, that work does not consider several aspects of the platform covered in our model, namely, the different types of components, the interaction between a running instance and the system, the R/W operation on a content provider, the semantics of the permission delegation mechanism and novel aspects of the security model, such as the management of runtime permissions.

Moving away from OS verification, many works have addressed the problem of relating inductively defined relations and executable functions, in particular in the context of programming language semantics. For instance, Tollitte *et al* [23]

show how to extract a functional implementation from an inductive specification in the `Coq` proof assistant. Similar approaches exist for Isabelle, see e.g. [7]. Earlier, alternative approaches such as [5,6] aim to provide reasoning principles for executable specifications.

6 Conclusion and future work

We have presented the development of an exhaustive formal specification of the Android security model that includes elements and properties that have been partially analyzed in previous work. We have enhanced the model considered in [8,9] with an explicit treatment of errors and with the latest version of the security mechanisms of the platform, which make it possible to grant permissions at run time. We also present the formalization of security properties concerning the Android permission mechanisms that have not previously been formally verified and proved. Using the programming language of the proof-assistant `Coq` we have defined a functional implementation of the reference validation mechanism, certified its correctness with respect to the axiomatic specification of the reference monitor and derived a certified `Haskell` prototype (`CertAndroidSec`) applying the program extraction mechanism provided by the proof assistant. In Appendix B, we provide listings of part of the `Haskell` code that has been automatically generated using `Coq`. The full certified code is available in [15]. The formal development is about 21k LOC of `Coq`, including proofs, and constitutes a suitable basis for reasoning about Android’s permission model and security mechanisms.

We plan to use the certified extracted algorithm as a testing oracle and also to conduct verification activities on actual implementations of the platform. In particular, we are investigating the use of that algorithm to compare the results of executing an action on a real Android platform and executing that same action on the correct program. This would allow us to monitor the actions performed in a real system and assessing whether the intended security policy is actually enforced by the particular implementation of the platform.

References

1. James P. Anderson. Computer Security technology planning study. Technical report, Deputy for Command and Management System, USA, 1972.
2. Android Developers. *Application Fundamentals*. Available at: <http://developer.android.com/guide/components/fundamentals.html> Access 09/17.
3. Android Developers. *Requesting Permissions at Run Time*. Available at: <https://developer.android.com/intl/es/training/permissions/requesting.html>. Access 09/17.
4. Android Developers. *R.styleable*. Available at: <http://developer.android.com/reference/android/R.styleable.html>. Access 09/17.

5. Antonia Balaa and Yves Bertot. Fix-point equations for well-founded recursion in type theory. In Mark Aagaard and John Harrison, editors, *TPHOLs*, volume 1869 of *LNCS*, pages 1–16. Springer, 2000.
6. G. Barthe, J. Forest, D. Pichardie, and V. Rusu. Defining and reasoning about recursive functions: A practical tool for the coq proof assistant. In *FLOPS*, volume 3945 of *LNCS*, pages 114–129. Springer, 2006.
7. Stefan Berghofer, Lukas Bulwahn, and Florian Haftmann. Turning inductive into equational specifications. In *TPHOL*, volume 5674 of *LNCS*, pages 131–146. Springer, 2009.
8. G. Betarte, J. D. Campo, C. Luna, and A. Romano. Verifying android’s permission model. In *ICTAC 2015 Proceedings*, volume 9399 of *LNCS*, pages 485–504. Springer, 2015.
9. G. Betarte, J. D. Campo, C. Luna, and A. Romano. Formal analysis of android’s permission-based security model,. *Sci. Ann. Comp. Sci.*, 26(1):27–68, 2016.
10. M. Bugliesi, S. Calzavara, and A. Spanò. Lintent: Towards security type-checking of android applications. In *Proceedings of FMOODS/FORTE 2013*, 2013.
11. Mauro Conti, Vu Thien Nga Nguyen, and Bruno Crispo. Crepe: context-related policy enforcement for android. In *Proceedings of ISC’10*, 2011.
12. A. Felt, H. Wang, A. Moshchuk, S. Hanna, and E. Chin. Permission re-delegation: Attacks and defenses. In *USENIX Security Symposium*, 2011.
13. E. Fragkaki, L. Bauer, L. Jia, and D. Swasey. Modeling and enhancing android’s permission system. In *Proceedings of ESORICS’12*, 2012.
14. Gartner. Gartner says worldwide sales of smartphones grew 9 percent in first quarter of 2017. Technical report, Gartner, Inc., 2017.
15. GSI. Formal verification of the security model of Android: Coq code. Available at: <http://www.fing.edu.uy/inco/grupos/gsi/documentos/proyectos/Android6-Coq-model.tar.gz>. Access 09/17.
16. P. Letouzey. *Programmation fonctionnelle certifiée – L’extraction de programmes dans l’assistant Coq*. PhD thesis, Université Paris-Sud, July 2004.
17. Pierre Letouzey. A New Extraction for Coq. In *Proceedings of TYPES’02*, volume 2646 of *LNCS*, 2003.
18. Mohammad Nauman, Sohail Khan, and Xinwen Zhang. Apex: extending android permission model and enforcement with user-defined runtime constraints. In *Proceedings of ASIACCS ’10*, 2011.
19. Open Handset Alliance. *Android project*. Available at: [//source.android.com/](http://source.android.com/). Access 09/17.
20. W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka. A formal model to analyze the permission authorization and enforcement in the android framework. In *Proceedings of the 2010 IEEE Second International Conference on Social Computing*, pages 944–951, Washington, DC, USA, 2010.
21. W. Shin, S. Kiyomoto, K. Fukushima, and T. Tanaka. A first step towards automated permission-enforcement analysis of the android framework. In *Proceedings of SAM 2010*, pages 323–329. CSREA Press, 2010.
22. The Coq Development Team. *The Coq Proof Assistant Reference Manual – Version V8.6*, 2016.
23. Pierre-Nicolas Tollitte, David Delahaye, and Catherine Dubois. Producing certified functional code from inductive specifications. In *CPP*, volume 7679 of *LNCS*, pages 76–91. Springer, 2012.

A Valid state

The model formalizes a notion of valid state that captures several well-formedness conditions. It is formally defined as a predicate *valid_state* on the elements of type `AndroidST`. This predicate holds on a state *s* if the following conditions are met:

- all the components both in installed applications and in system applications have different identifiers;
- no component belongs to two different applications present in the device;
- no running component is an instance of a content provider;
- every temporally delegated permission has been granted to a currently running component and over a content provider present in the system;
- every running component belongs to an application present in the system;
- every application that sets a value for a resource is present in the system;
- the domains of the partial functions `Manifests`, `Certs` and `AppDefPS` are exactly the identifiers of the user installed applications;
- the domains of the partial functions `AppPS` and `PermsGr` are exactly the identifiers of the applications in the system, both those installed by the users and the system applications;
- every installed application has an identifier different to those of the system applications, whose identifiers differ as well;
- all the permissions defined by applications have different identifiers;
- every partial function is indeed a function, that is, their domains don't have repeated elements;
- every individually granted permission is present in the system; and
- all the sent intents have different identifiers.

All these safety properties have a straightforward interpretation in our model. We omit here the formal definition of *valid_state* due to space constraints. The full formal definition of the predicate is available in [15].

B Generated code

Just for the sake of illustration, in what follows we provide listings of part of the Haskell code that has been automatically generated using the Coq extraction mechanism. The code is annotated with inline comments and manually indented to fit on the page width.

We have included the definition of the `System`, as a datatype and the complete definition of the action `install` and the code of the dispatcher, which implements the execution of an action in a given state.

Listing 1.1. The System

```

{- The System is represented as a datatype
   - comprising a State and an Environment
   -}

data System =
  Sys State Environment

-- The Environment datatype
data Environment =
  Env
  -- The manifest and certificate of installed user applications
  (Mapping IdApp Manifest)
  (Mapping IdApp Cert)
  -- The permissions defined by the applications
  (Mapping IdApp ([] Perm0))
  -- System applications
  ([] SysImgApp)

-- The datatype State
data State =
  St
  -- The installed user applications
  ([] IdApp)
  -- Granted group and individual permissions for each application
  (Mapping IdApp ([] IdGrp))
  (Mapping IdApp ([] Perm0))
  -- Running components and their instances
  (Mapping ICmp Cmp)
  -- Permanent and temporary permission delegations
  (Mapping ((,) ((,) IdApp CProvider) Uri) PType)
  (Mapping ((,) ((,) ICmp CProvider) Uri) PType)
  -- Values of resources
  (Mapping ((,) IdApp Res) Val)
  -- Sent intents
  ([] ((,) ICmp Intent0))

```

Listing 1.2. Install checks

```

{- Install semantics:
   - install_pre checks whether an installation can take place in a state.
   - It returns the corresponding ErrorCode if the installation is not allowed
   -}

install_pre :: IdApp -> Manifest -> Cert -> ([] Res) ->
  System -> Prelude.Maybe ErrorCode
install_pre app0 m c lRes s =
-- The application can not be already installed
  case isAppInstalledBool app0 s of {
    Prelude.True -> Prelude.Just App_already_installed;
    Prelude.False ->
-- Components in the application must have different identifiers
    case has_duplicates idCmp_eq (map getCmpId (cmp m)) of {
      Prelude.True -> Prelude.Just Duplicated_cmp_id;
      Prelude.False ->
-- The defined permissions must have different identifiers.
      case has_duplicates idPerm_eq (map idP (usrP m)) of {
        Prelude.True -> Prelude.Just Duplicated_perm_id;
        Prelude.False ->
-- The new components' ids must differ from those already present in the system.
        case existsb (\c0 -> cmpIdInStateBool c0 s) (cmp m)
        of {
          Prelude.True -> Prelude.Just Cmp_already_defined;
          Prelude.False ->
-- No permission defined by other application can be redefined.
          case Prelude.not (authPermsBool m s) of {
            Prelude.True -> Prelude.Just
              Perm_already_defined;
            Prelude.False ->
-- All the intent filters must be well defined.
            case anyDefinesIntentFilterIncorrectly (cmp m)
            of {
              Prelude.True -> Prelude.Just
                Faulty_intent_filter;
              Prelude.False -> Prelude.Nothing}}}}}

```

Listing 1.3. Install effect

```

{- The function install_post compute the state resulting from
   - installing a fresh application
   -}

install_post :: IdApp -> Manifest -> Cert -> ([[]] Res) ->
  System -> System
install_post app0 m c lRes s =
  let {oldstate = state s} in
  let {oldenv = environment s} in
  -- The application identifier is appended to the list of installed applications
  Sys (St (:) app0 (apps oldstate))
  -- with no permission or permission groups granted,
  (map_add idApp_eq (grantedPermGroups oldstate) app0 ([[]])
  (map_add idApp_eq (perms oldstate) app0 ([[]]) (running
  oldstate)
  (delPPerms oldstate) (delTPerms oldstate)
  -- its resources are initialized with the default value, and
  (addNewResCont app0 (resCont oldstate) lRes) (sentIntents
  oldstate))
  -- its manifest, certificate and permissions are stored in the state.
  (Env
  (map_add idApp_eq (manifest oldenv) app0 m)
  (map_add idApp_eq (cert oldenv) app0 c)
  (map_add idApp_eq (defPerms oldenv) app0 (nonSystemUsrP m))
  (systemImage oldenv))

```

Listing 1.4. Safe install

```

{- The function install_safe checks for errors using the function install_pre,
   - returning the state unmodified along with the error code, if there is one.
   - Otherwise, it computes the new state by executing install_post
   -}

install_safe :: IdApp -> Manifest -> Cert -> ([[]] Res) -> System -> Result0
install_safe app0 m c lRes s =
  case install_pre app0 m c lRes s of {
    Prelude.Just ec -> Result (Error0 ec) s;
    Prelude.Nothing -> Result Ok (install_post app0 m c lRes s)}

```

Listing 1.5. Dispatcher

```

{- The function step is just a dispatcher which
   - performs pattern matching on the action to be
   - executed and calls the corresponding function
   - (for example, install_safe)
   -}

step :: System -> Action -> Result0
step s a =
  case a of {
    Install app0 m c lRes -> install_safe app0 m c lRes s;
    Uninstall app0 -> uninstall_safe app0 s;
    Grant p app0 -> grant_safe p app0 s;
    Revoke p app0 -> revoke_safe p app0 s;
    GrantPermGroup grp app0 -> grantgroup_safe grp app0 s;
    RevokePermGroup grp app0 -> revokegroup_safe grp app0 s;
    HasPermission a0 p -> Result Ok s;
    Read0 ic cp u -> read_safe ic cp u s;
    Write0 ic cp u v -> write_safe ic cp u v s;
    StartActivity intt ic -> startActivity_safe intt ic s;
    StartActivityForResult intt n ic -> startActivity_safe intt ic s;
    StartService intt ic -> startService_safe intt ic s;
    SendBroadcast intt ic p -> sendBroadcast_safe intt ic p s;
    SendOrderedBroadcast intt ic p -> sendBroadcast_safe intt ic p s;
    SendStickyBroadcast intt ic -> sendStickyBroadcast_safe intt ic s;
    ResolveIntent intt a0 -> resolveIntent_safe intt a0 s;
    ReceiveIntent intt ic a0 -> receiveIntent_safe intt ic a0 s;
    Stop ic -> stop_safe ic s;
    GrantP ic cp a0 u pt -> grantP_safe ic cp a0 u pt s;
    RevokeDel ic cp u pt -> revokeDel_safe ic cp u pt s;
    Call ic sac -> call_safe ic sac s }

```
