Differential Verification of Information Flow in SEAndroid Policies

Differential Verification of Information Flow in SEAndroid Policies

Lorenzo Ceragioli, Letterio Galletta, and Edoardo Lunati

IMT School for Advanced Studies Lucca, Lucca, Italy

Abstract. SEAndroid is deployed on almost all modern Android devices to enforce mandatory access control. The Android Open Source Project regularly publishes a predefined SEAndroid policy that each vendor customises for its devices. These customisations and policy updates may cause security regressions: even small misconfigurations may introduce new information flows leading to exploitable vulnerabilities. We propose a differential verification framework that determines whether security-relevant changes between two SEAndroid configurations affect information-flow properties as intended. Our verification framework is based on the novel comparative modal logic *CML* interpreted over pairs of Kripke structures. We formalise SEAndroid policies within this logic and define a suitable model-checking algorithm for differential reasoning. We implement our framework in the tool *Mordente*, and evaluate it on real-world SEAndroid policies.

Keywords: Comparative modal logic · Policy evolution analysis · Access control.

1 Introduction

Android is currently the most widely used operating system for mobile devices, making it a frequent target of privilege escalation and code execution attacks [7, 17]. Typically, these attacks aim to compromise high-privileged system daemons, often bypassing the traditional discretionary access control of Linux systems [7]. To mitigate such threats, Security Enhancements for Android (SEAndroid), based on SELinux [2], introduces mandatory access control into the Android platform. SEAndroid is integrated into the kernel and checks every action performed by a subject (e.g., a process) over an object (e.g., a file or socket). In SEAndroid, subjects and objects are associated with abstract security labels as specified in a labelling policy. In addition, a permission policy lists the operations that a labelled subject may perform on a labelled object (all others being denied by default). The Android Open Source Project (AOSP) continuously updates a default SEAndroid policy, which the Android Original Equipment Manufacturers (OEMs) further customise for their devices. Given the size and evolving nature of the Android codebase, ensuring that the SEAndroid configuration enforces the intended security properties is a challenging task [11]. Additionally, modifications to the permission and labelling policies affect the

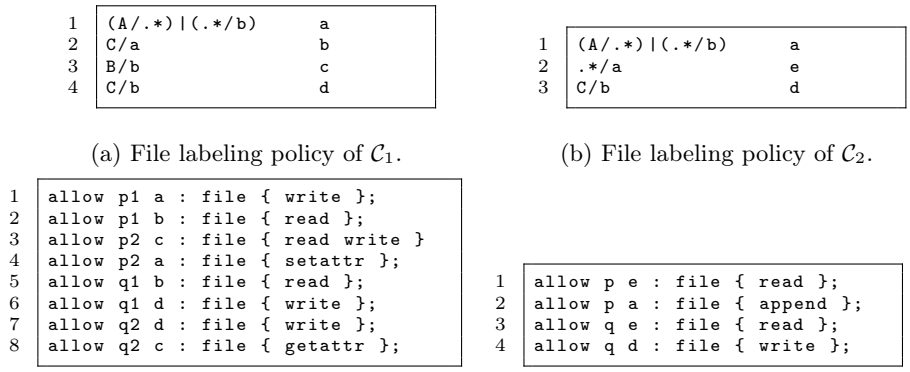
system's effective security posture, and both AOSP and OEMs have introduced misconfigurations and vulnerabilities in the past [14].

Previous work has investigated the security of SEAndroid and SELinux policies, proposing tools for visualisation, inspection, and static verification [5, 9, 10, 12, 15]. These tools formalise security in terms of information flow, a well-established approach for reasoning about integrity, confidentiality, and isolation. In practice, we say that there is an information flow from file f to file f' if some processes $p_1, p_2, \ldots, p_n$ and files $f_1, f_2, \ldots, f_{n+1}$ exist such that the process p_i reads from f_i and writes on f_{i+1}, with $f_1 = f$ and $f_{n+1} = f'$. Several important security properties for Android systems can be stated in terms of information flow. For example, to avoid privilege escalation, we can impose that low-privileged domains, such as `untrusted_app`, can never write to `system_file`, `exec_file`, or `shared_libs_file`. Moreover, to enforce cross-app isolation, we may prohibit `untrusted_app` or `platform_app` from interacting with `app_data_file` belonging to other applications. However, existing tools provide little support for comparing configurations across versions or vendors in terms of their security properties. Additionally, they do not help analysts preserve security properties when they are undocumented, which is often the case in real-world policies.

To address this gap, we propose a differential verification framework that determines whether security-relevant changes between two SEAndroid configurations alter information-flow properties as intended. Our framework is based on the new *comparative modal logic CML*, interpreted over sets of Kripke structures representing different system versions. *CML* extends classical logic with three classes of operators: (*i*) two forward modalities $\Diamond$ ("for some next state") and $\Box$ ("for all next states"); (*ii*) two backward modalities $\blacklozenge$ ("for some previous state") and $\blacksquare$ ("for all previous states"); (*iii*) a version operator $\uparrow_i$ used to refer to the i-th version of the system, represented by the i-th Kripke structure. A peculiarity of *CML* is that, to decide the validity of a formula where two operators $\uparrow_i$ and $\uparrow_j$ occur (with $i \neq j$), the properties stated in terms of two different Kripke structures must be compared. We do this by enriching each of our Kripke structures with an interpretation over a common set Ω of concrete states.

To use *CML* for differential reasoning over SEAndroid policies, we first compute a relation describing the information flows between file labels permitted by each policy. The Kripke model of an SEAndroid configuration consists of file labels, the corresponding information-flow relation, and a state annotation capturing relevant security properties. In the context of SEAndroid, the set Ω of concrete states contains all the file paths, and the interpretation of Kripke structures derives from the labelling policy: file labels are assigned to file paths by matching regular expressions. This allows us to relate abstract labels to actual filesystem objects and reason about information flows in the system. Finally, we implement our framework in the tool *Mordente*, available at [1], and evaluate it on real-world SEAndroid policies of different vendors and versions.

To the best of our knowledge, our work is the first proposal comparing different versions of SEAndroid policies in terms of their information flow, taking



(a) File labeling policy of $\mathcal{C}_1$.

(b) File labeling policy of $\mathcal{C}_2$.

(c) Access control policy of $\mathcal{C}_1$.

(d) Access control policy of $\mathcal{C}_2$.

Fig. 1: Two examples of SEAndroid configurations.

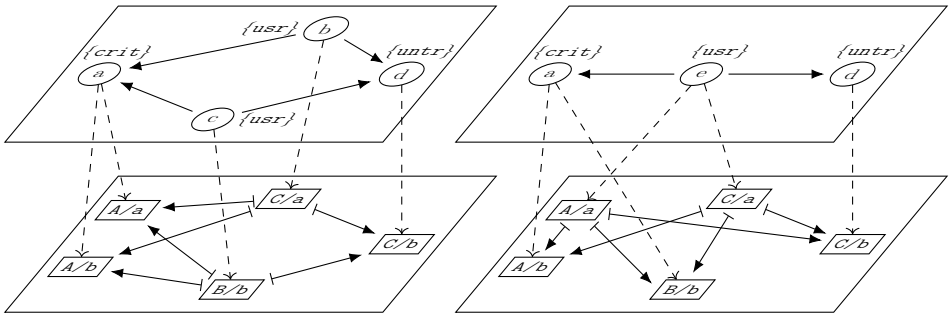
into account the changes in the two labelling policies. A key advantage of our approach over other tools for regression verification is that it does not require the policy analyst to provide a complete specification of the desired security properties. We can ensure that changing from one SEAndroid version to another only impacts the needed portion of the system, while the remaining part preserves all its properties, including those not explicitly documented by the developers.

***Mordente* at Work** Consider the two SEAndroid configurations $\mathcal{C}_1$ and $\mathcal{C}_2$ of Figure 1. Each configuration consists of two components: a *labelling policy* (above in the figure) and a *permission policy* (below in the figure).

The labelling policy is stored in a so-called *file-context* and consists of a sequence of rules mapping regular expressions of filesystem paths to the security context that labels them. Security contexts usually consist of a user, a role, and a type, but for simplicity, we consider only the type component, which is the most relevant in Android (being type enforcement the primary access control mechanism in mobile devices); thus, hereafter, we treat labels as consisting solely of types. For example, in Figure 1a the rule on line 1 assigns label `a` to all files in the directory `A` and to any file named `b`, while line 3 assigns `c` to just the file at path `B/b`. Note that the order of rules matters, and SEAndroid applies the last-matched one (regexes matching smaller languages are usually at the end of file contexts). Thus, `B/b` is associated with `c` (line 3) and not with `a` (line 1).

The permission policy specifies which operations labelled subjects are allowed to perform on labelled objects. Administrators typically specify configurations using SELinux's kernel policy language [4], which is then compiled to a kind of (kernel binary) access-control matrix. As illustrated in Figure 1a, the permission policy is essentially a sequence of rules of the following form.

```
allow subject_type object_type : class {permissions}
```



(a) File information flow in $\mathcal{C}_1$. (b) File information flow in $\mathcal{C}_2$.

Fig. 2: Kripke structures of two SEAndroid configurations: solid arrows represent information flows, dashed arrows represent file labelling.

For instance, the rule on line 1 permits subjects labelled `p1` writing files labeled `a`. Any operation not explicitly allowed is denied by default. Permission policies may also contain `neverallow` rules, attributes that group related types under shared behavioural constraints, and macros that expand into commonly used sets of permissions. The full policy language is outside the scope of this paper, as it is used only for examples, since our tool operates on compiled policies.

In order to compare the two configurations of Figure 1, we first give them a semantics in terms of Kripke structures (see Figure 2) where states represent file labels, and arcs the information flow between them induced by *read* and *write* operations (or similar ones like *getattr* and *setattr*). Then, we encode security properties using three atomic propositions: `crit` (i.e. *critical*, is associated with `a` both in $\mathcal{C}_1$ and $\mathcal{C}_2$), `untr` (i.e. *untrusted*, is associated with `d` both in $\mathcal{C}_1$ and $\mathcal{C}_2$) and `usr` (i.e. *user*, is associated with all the remaining labels). Note that label names differ in the two configurations, and the common ones may have a different meaning (like `a`). Therefore, in order to compare the semantics of the two configurations, their labels must be concretised in terms of actual file paths. This is achieved through the file labelling policies: for each policy, we evaluate the labels while preserving the edges, obtaining the graphs below in Figure 2.

Using *Mordente*, the policy administrator can build these transition systems automatically, and can check the validity of the following *CML* proposition ϕ, stating that all the files that used to affect some untrusted file in $\mathcal{C}_1$ satisfy `usr` in $\mathcal{C}_2$, and they still influence the same files of the previous version.

$$\phi = \uparrow_1(\Diamond \texttt{untr}) \Rightarrow \uparrow_2(\texttt{usr} \wedge \Diamond \uparrow_1 \texttt{untr})$$

The tool signals that the ϕ is not satisfied by the version update, informing that the files labelled as `c` in $\mathcal{C}_1$ and as `a` in $\mathcal{C}_2$ contradict the property, e.g. the concrete file path `B/b`. Note indeed that in Figure 2a, the file at path `B/b` accesses `C/b`, which is untrusted, while the same access is not possible in Figure 2b.

Synopsis In Section 2, we define *CML* and its model checking. Section 3 encodes SEAndroid using our logic. Section 4 presents *Mordente* and its experimental evaluation. In Sections 5 and 6, we compare our approach with the literature and draw some conclusions. Appendices contain formal proofs and test details.

2 A Comparative Modal Logic

We define Comparative Modal Logic (*CML*), a logic for comparing different versions of the same system, each represented as a transition system with states labelled by the properties of interest (a Kripke structure). In the following, we let $\mathbb{I}$ be the finite set of version names, and $\mathbb{P}$ the set of atomic propositions.

Definition 1 (*CML* Proposition). *A CML proposition $\phi \in \Phi$ is defined by the following grammar, with $i \in \mathbb{I}$ a version name and $p \in \mathbb{P}$ an atomic proposition.*

$$\phi ::= \mathit{true} \mid p \mid \phi \wedge \phi \mid \neg\phi \mid \uparrow_i \phi \mid \Diamond\phi \mid \blacklozenge\phi$$

Intuitively: *true* is always satisfied; p tells that the atomic proposition p is satisfied; $\uparrow_i \phi$ is satisfied if ϕ is satisfied in the version i; $\Diamond\phi$ is satisfied if ϕ is satisfied in at least a next state; $\blacklozenge\phi$ is satisfied if ϕ is satisfied in at least a previous state; boolean conjunction and negation behaves as expected.

We derive other logical operators in the usual way.

$$\Box\phi = \neg\Diamond\neg\phi \qquad \blacksquare\phi = \neg\blacklozenge\neg\phi \qquad \phi \vee \psi = \neg(\neg\phi \wedge \neg\psi) \qquad \phi \Rightarrow \psi = \neg\phi \vee \psi$$

Example 1. The formula $\uparrow_1(\mathtt{a} \wedge \Diamond(\neg\mathtt{b} \wedge \uparrow_2 \mathtt{b}))$ is satisfied if a is valid in the first version, and we can access some state where b is valid only in the second version.

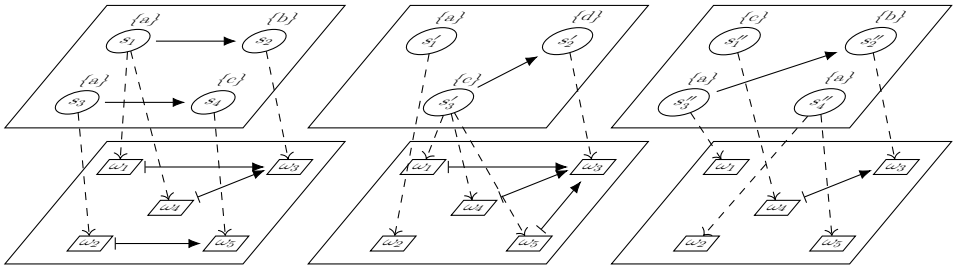
To give a formal semantics to *CML*, we start by defining a model for versions.

Definition 2 (Kripke Structure). *A* Kripke structure *is a triple $\mathcal{K} = (S, \rightarrow, \vdash)$ with S a set of states; $\rightarrow \subseteq S \times S$ the transition relation; and where $\vdash \subseteq S \times \mathbb{P}$ associates atomic propositions with states in which they hold.*

The purpose of *CML* is to compare different versions, and for that we need a common ground, which is represented by the special set of states $\Omega \ni \omega, \omega', \ldots$ that we assume to be *concrete states*. The states of any version can be thought of as abstract names for classes of concrete states.

Definition 3 (State Evaluation). *A* state evaluation *for a set of states S is a function $\downarrow\colon S \longrightarrow 2^{\Omega}$ that associates each state with the concrete ones it represents, and it satisfies that $\downarrow(s) \cap \downarrow(s') = \emptyset$ if $s \neq s'$, and $\bigcup_{s \in S} \downarrow(s) = \Omega$.*

As a result of that, the Kripke structure of a version $\mathcal{K}$ can always be seen as an abstract representation of a Kripke structure over the set of concrete states: its concretisation is obtained by evaluating states according to the given function.



(a) Version 1. (b) Version 2. (c) Version 3.

Fig. 3: A *CML* model of example and the concretization its components.

Definition 4 (Concretization). *Given a Kripke structure $\mathcal{K} = (S, \longrightarrow, \vdash)$ and a state evaluation $\downarrow$ for S, the concretization of $\mathcal{K}$ with respect to $\downarrow$ is a Kripke structure $(\Omega, \mapsto, \Vdash)$ with*

- *$\mapsto \subseteq \Omega \times \Omega$ such that $\omega \mapsto \omega'$ if and only if $s \longrightarrow s'$ for some s and s' in S with $\omega \in \downarrow(s)$ and $\omega' \in \downarrow(s')$;*
- *$\Vdash \subseteq \Omega \times \mathbb{P}$ such that $\omega \Vdash p$ if and only if $\omega \in \downarrow(s)$ and $s \vdash p$ for some $s \in S$.*

A *CML* model is a set of Kripke structures paired with state evaluations.

Definition 5 (Model). *A CML model $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i \in \mathbb{I}}$ is a collection of pairs indexed by the set $\mathbb{I}$ of versions, where $\mathcal{K}_i = (S_i, \longrightarrow_i, \vdash_i)$ is the Kripke structure of the version i, and $\downarrow_i \colon S_i \longrightarrow 2^{\Omega}$ is its state evaluation.*

Example 2. Let $\Omega = \{\omega_1, \omega_2, \omega_3, \omega_4, \omega_5\}$. The *CML* model in Figure 3 is $\mathcal{M} = \{(\mathcal{K}_1, \downarrow_1), (\mathcal{K}_2, \downarrow_2), (\mathcal{K}_3, \downarrow_3)\}$, where, e.g., the graph above in Figure 3b represents $\mathcal{K}_2 = (\{s'_1, s'_2, s'_3\}, \{(s'_3, s'_2)\}, \{(s'_1, a), (s'_2, d), (s'_3, c)\})$, while the graph below is its concretisation with respect to the state evaluation represented by the vertical dashed arrows, $\downarrow_2 = \{(s'_1, \{\omega_2\}), (s'_2, \{\omega_3\}), (s'_3, \{\omega_1, \omega_4, \omega_5\})\}$.

We now define the validity of a formula according to a *CML* model. By expressing it in terms of common, concrete states, we allow for comparing different versions.

Definition 6. *Given a CML model $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i \in I}$, we define the validity of a CML proposition $\phi \in \Phi$ with respect to a concrete state $\omega \in \Omega$ and a version $i \in I$ though the following satisfaction relation $\omega, i \models_{\mathcal{M}} \phi$:*

$$
\begin{array}{ll}
\omega, i \models_{\mathcal{M}} \mathit{true} & \\
\omega, i \models_{\mathcal{M}} p & \text{if } \omega \Vdash_i p \\
\omega, i \models_{\mathcal{M}} \phi \wedge \phi' & \text{if } \omega, i \models_{\mathcal{M}} \phi \text{ and } \omega, i \models_{\mathcal{M}} \phi' \\
\omega, i \models_{\mathcal{M}} \neg\phi & \text{if } \omega, i \not\models_{\mathcal{M}} \phi \\
\omega, i \models_{\mathcal{M}} \uparrow_j \phi & \text{if } \omega, j \models_{\mathcal{M}} \phi \\
\omega, i \models_{\mathcal{M}} \Diamond\phi & \text{if } \omega' \text{ exists such that } \omega \mapsto_i \omega' \text{ and } \omega', i \models_{\mathcal{M}} \phi \\
\omega, i \models_{\mathcal{M}} \blacklozenge\phi & \text{if } \omega' \text{ exists such that } \omega' \mapsto_i \omega \text{ and } \omega', i \models_{\mathcal{M}} \phi
\end{array}
$$

where $(\Omega, \mapsto_i, \Vdash_i)$ *is the concretisation of* $\mathcal{K}_i$ *with respect to* $\downarrow_i$.

We say that a concrete state $\omega \in \Omega$ *satisfies a CML proposition* ϕ*, and we write* $\omega \models_{\mathcal{M}} \phi$*, if* $\omega, i \models_{\mathcal{M}} \phi$ *for any* $i \in \mathbb{I}$*. Finally, we say that the CML model* $\mathcal{M}$ *satisfies* ϕ*, and we write* $\mathcal{M} \models \phi$*, if* $\omega \models_{\mathcal{M}} \phi$ *for any* $\omega \in \Omega$.

Example 3. Consider the *CML* model $\mathcal{M}$ of Example 2 and assume that we want to preserve some property while passing from version i to j. The property encoded by the atomic predicate a is preserved if $\uparrow_i \mathtt{a} \Rightarrow \uparrow_j \mathtt{a}$, i.e. if all concrete states satisfying `a` in the first version also satisfy it in the second one. For example $\mathcal{M} \models \uparrow_3 \mathtt{a} \Rightarrow \uparrow_1 \mathtt{a}$, while $\mathcal{M} \not\models \uparrow_1 \mathtt{a} \Rightarrow \uparrow_3 \mathtt{a}$ (the state ω_4 is a counterexample).

The preservation of reachability is more involved: various *CML* propositions can be used, with different nuances in their meaning. Consider the following predicates, noting that $\uparrow_i(\mathtt{a} \wedge \Diamond \mathtt{b})$ is satisfied by concrete states that used to satisfy `a` and to access states that used to satisfy `b`:

$\phi_{i,j} = \uparrow_i(\mathtt{a} \wedge \Diamond \mathtt{b}) \Rightarrow \uparrow_j(\mathtt{a} \wedge \Diamond \mathtt{b})$ specifies that such states still satisfy `a` and can access states satisfying `b` now;

$\psi_{i,j} = \uparrow_i(\mathtt{a} \wedge \Diamond \mathtt{b}) \Rightarrow \uparrow_j(\uparrow_i \mathtt{a} \wedge \Diamond \uparrow_i \mathtt{b})$ means that they replicate the accessibility of the previous version, but says nothing about satisfying atomic predicates;

$\xi_{i,j} = \uparrow_i(\mathtt{a} \wedge \Diamond \mathtt{b}) \wedge \uparrow_j \mathtt{a} \Rightarrow \uparrow_j \Diamond \mathtt{b}$ requires only states that currently satisfy `a` to replicate the accessibility of the previous version.

Then, $\mathcal{M}$ satisfies $\psi_{1,2}$, $\xi_{1,2}$ and $\xi_{1,3}$ (see Figure 3), but not $\phi_{1,2}$ nor $\phi_{1,3}$ (ω_4 does not satisfy a in $\mathcal{K}_2$ nor $\mathcal{K}_3$), and not $\psi_{1,3}$ (ω_1 does not access ω_3 in $\mathcal{K}_3$).

We now investigate the model-checking problem, namely, given a model $\mathcal{M}$ and a *CML* proposition ϕ, we want to check if $\omega \models_{\mathcal{M}} \phi$ for any $\omega \in \Omega$. Ideally, we want to compute the satisfaction set $\{\omega \in \Omega \mid \omega \models_{\mathcal{M}} \phi\}$, but Ω is often considerably large (even infinite in theory): we need a feasible way of computing a succinct representation of the satisfaction set in terms of the (finite and possibly small) sets of states S_i.

We start by defining a normal form for *CML* where $\uparrow_i$ appears only before modal operators and atomic propositions, and before each of them. Formally:

Definition 7 (Normal Form). *CML propositions in* normal form *are generated by the following grammar, with* $i \in \mathbb{I}$ *a version and* $p \in \mathbb{P}$ *atomic proposition.*

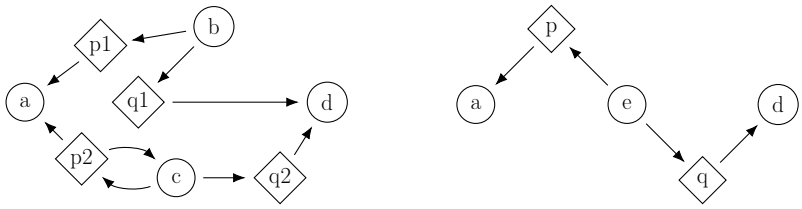
$$\phi ::= \mathit{true} \mid \phi \wedge \phi \mid \neg\phi \mid \uparrow_i p \mid \uparrow_i \Diamond \phi \mid \uparrow_i \blacklozenge \phi$$

We let $\Phi^\bullet \subsetneq \Phi$ *be the set of CML propositions in normal form.*

Each *CML* proposition can be transformed into an equivalent normal form.

Theorem 1. *For each CML proposition* ϕ*, there exists a CML proposition in normal form* $\phi^\bullet$ *such that* $\omega \models_{\mathcal{M}} \phi$ *if and only if* $\omega \models_{\mathcal{M}} \phi^\bullet$ *for any* ω *and* $\mathcal{M}$.

We define compatible states, i.e. functions associating a state to each version i such that it is possible to be in all of the states at the same time. We write $\bar{s}$ for a function from versions to states, and $\bar{s}[i]$ for the state associated with $i \in \mathbb{I}$.



(a) Information flow relation of $\mathbb{A}_1$. (b) Information flow relation of $\mathbb{A}_2$.

Fig. 4: Information flow relation of two configurations: circles and diamonds are file and non-file labels respectively, we omit the arcs obtained by transitivity.

Definition 8 (Compatible State). *Given a CML model* $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i\in\mathbb{I}}$ *with* $\mathcal{K}_i = (S_i, \longrightarrow_i, \vdash_i)$ *for all* $i \in \mathbb{I}$*, a* compatible state *of* $\mathcal{M}$ *is a function* $\bar{s}$ *associating a version* $i \in \mathbb{I}$ *with a state* $s \in S_i$ *such that* $\bigcap_{i\in I} \downarrow_i \bar{s}[i] \neq \emptyset$*. Let* $\mathbb{S}$ *be the set of all compatible states.*

We finally define the succinct representation for the satisfaction set of a *CML* proposition. More precisely, given ϕ, we compute the set of compatible states $\bar{s}$ that correspond to concrete states satisfying ϕ. The definition is given by recursion, immediately suggesting a model-checking procedure.

Definition 9 (Compatible Satisfaction Set). *Given a CML model* $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i\in I}$ *with* $\mathbb{S}$ *its set of compatible states and* $\mathcal{K}_i = (S_i, \longrightarrow_i, \vdash_i)$ *for all* $i \in I$*, and given* $\phi \in \Phi^\bullet$*, we let the* compatible satisfaction set *of* ϕ *with respect to* $\mathcal{M}$ *be* $[\![\phi]\!] \subseteq \mathbb{S}$ *recursively defined as follows:*

$$[\![true]\!] = \mathbb{S} \qquad [\![\neg\phi]\!] = \mathbb{S} \setminus [\![\phi]\!] \qquad [\![\phi \wedge \phi']\!] = [\![\phi]\!] \cap [\![\phi']\!]$$
$$[\![\uparrow_i p]\!] = \{\bar{s} \in \mathbb{S} \mid \bar{s}[i] \vdash_i p\} \qquad [\![\uparrow_i \Diamond\phi]\!] = \{\bar{s} \mid \bar{s}' \in [\![\phi]\!] \text{ exists s.t. } \bar{s}[i] \longrightarrow_i \bar{s}'[i]\}$$
$$[\![\uparrow_i \blacklozenge\phi]\!] = \{\bar{s} \mid \bar{s}' \in [\![\phi]\!] \text{ exists s.t. } \bar{s}'[i] \longrightarrow_i \bar{s}[i]\}$$

The following result guarantees the correctness of the compatible satisfaction set with respect to the satisfaction relation of *CML*.

Theorem 2. *Given a CML model* $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i\in I}$*, it holds for all* $\omega \in \Omega$ *and* $\phi \in \Phi^\bullet$ *that* $\omega \models_{\mathcal{M}} \phi$ *if and only if* $\omega \in \bigcup_{\bar{s}\in[\![\phi]\!]} \bigcap_{i\in I} \downarrow_i \bar{s}[i]$

3 Representing SEAndroid Policies

In the following, we let Ω be the set of legal file paths of Android devices. As it is clear from the notation, files will be the concrete states for our *CML* encoding. We also let $\Sigma \supsetneq \Omega$ be the set of all possible entities of an Android system: files, processes, ports. We denote with $\mathbb{L}$ and $\mathbb{L}_{\mathtt{f}} \subsetneq \mathbb{L}$ the sets of all SEAndroid labels and of those associated with files, respectively; $\ell_\perp \in \mathbb{L}_{\mathtt{f}}$ is the distinguished *default* file label used when no other labels can be associated

(usually `default_t`). We assume O to be the set of operations controlled by SEAndroid (reading files, searching in directories, etc). Finally, we let $\mathbb{P}$ be the set of properties appearing in security policies, which we will use as atomic propositions in the *CML* encoding.

A SEAndroid configuration has two main components: a set of permitted operations between labelled entities and a list of rules for associating files with labels. In addition, we consider a security policy annotating labels with their security properties, such as secrecy or trust level.

Definition 10 (SEAndroid Configuration). *A* SEAndroid configuration $\mathcal{C}$ *is a triple* $(\mathbb{A}, \mathbb{F}, \Gamma)$ *where*

- *the* access control policy $\mathbb{A}$ *is a finite set of triples* $(\ell, o, \ell') \in \mathbb{L} \times O \times \mathbb{L}$*;*
- *the* file labeling policy $\mathbb{F}$ *is a list of pairs* $(\mathcal{L}, \ell)$ *with* $\mathcal{L} \subseteq 2^{\Omega}$ *a regular language of file paths and* $\ell \in \mathbb{L}_{\mathtt{f}}$ *a file label.*
- *the* security policy $\Gamma \subseteq \mathbb{L}_{\mathtt{f}} \times \mathbb{P}$ *associates labels with predicates in* $\mathbb{P}$*.*

Example 4. Consider the configurations $\mathcal{C}_1 = (\mathbb{A}_1, \mathbb{F}_1, \Gamma_1)$ and $\mathcal{C}_2 = (\mathbb{A}_2, \mathbb{F}_2, \Gamma_2)$ of Figure 1. We interpret each line in SELinux notation `allow b a : file { write };` of the access control policies (below) as a triple $(\mathtt{b}, \mathtt{file\ write}, \mathtt{a})$. The file labelling policies (above) are lists of pairs, where languages are expressed as regular expressions. In accordance with Android behaviour, we read the files bottom-up, thus taking a list in reverse order with respect to what is in Figure 1. The security policies are $\Gamma_1 = \{(a, \mathtt{crit}), (b, \mathtt{usr}), (c, \mathtt{usr}), (d, \mathtt{untr})\}$ and $\Gamma_2 = \{(a, \mathtt{crit}), (e, \mathtt{usr}), (d, \mathtt{untr})\}$.

We assume an information flow evaluation function $\mathit{ife} : O \to 2^{\{\triangleright, \triangleleft\}}$ associating each operation o with the directions of the information flows it causes: $\triangleright \in \mathit{ife}(o)$ if o allows the process to send information to the object on which o is performed; $\triangleleft \in \mathit{ife}(o)$ if o allows the process to receive information from it. It is now possible to represent the information flow resulting from a policy.

Definition 11 (Information Flow Relation). *The* information flow relation I *of a SEAndroid access control policy* $\mathbb{A}$ *is the smallest subset of* $\mathbb{L} \times \mathbb{L}$ *such that:*

- *if* $(\ell, o, \ell') \in \mathbb{A}$ *for some* o *with* $\triangleright \in \mathit{ife}(o)$ *then* $(\ell, \ell') \in I$*;*
- *if* $(\ell', o, \ell) \in \mathbb{A}$ *for some* o *with* $\triangleleft \in \mathit{ife}(o)$ *then* $(\ell, \ell') \in I$*;*
- *if* $(\ell, \ell'') \in I$ *and* $(\ell'', \ell') \in I$ *then* $(\ell, \ell') \in I$*.*

Computing the Kripke structure of an SEAndorid configuration amounts to considering the information flow relation over file labels only, and to associate such labels with atomic propositions according to the security policy Γ.

Definition 12 (Kripke Encoding). *The Kripke structure of a SEAndroid configuration* $(\mathbb{A}, \mathbb{F}, \Gamma)$ *with information flow relation* I *is* $(\mathbb{L}_{\mathtt{f}}, I \cap (\mathbb{L}_{\mathtt{f}} \times \mathbb{L}_{\mathtt{f}}), \Gamma)$.

Example 5. The graphs above in Figure 2 represent the Kripke models of the two configurations $\mathcal{C}_1$ and $\mathcal{C}_2$ of Figure 1. The transitions are obtained as the subset over file labels of the information flow relations depicted in Figure 4; atomic propositions are associated according to the security policies Γ_1 and Γ_2.

Given $\mathbb{F}$, the file labelling policy of the SEAndroid configuration, we define $\lambda_{\mathbb{F}}$ to be the function used by the operating system to associate labels with files. Intuitively, given a file with path ω, the rules of $\mathbb{F}$ are processed sequentially (i.e. in reverse order with respect to the file context). For each pair $(\mathcal{L}, \ell)$, the regular expression representing $\mathcal{L}$ is considered: if $\omega \in \mathcal{L}$, the label ℓ is associated with ω, otherwise the process moves to the next pair.

Definition 13 (File Labeling Function). *The* file labeling function $\lambda_{\mathbb{F}} \colon \Omega \longrightarrow \mathbb{L}_{\mathtt{f}}$ *of the file labeling policy* $\mathbb{F}$ *is defined as* $\lambda_{\mathbb{F}}(\omega) = \ell$ *if* $(\mathcal{L}, \ell)$ *is the first pair in* $\mathbb{F}$ *such that* $\omega \in \mathcal{L}$*, and* $\lambda_{\mathbb{F}}(\omega) = \ell_\perp$ *if no* $\mathcal{L}$ *of* $\mathbb{F}$ *contains* ω*.*

Example 6. The file labeling functions of $\mathcal{C}_1$ and $\mathcal{C}_2$ in Figure 1 follow, where $\mathcal{L}_a$ and $\mathcal{L}_e$ are the languages recognized by `(A/.*)|(.*/b)` and `.*/a`, respectively.

$$\lambda_{\mathbb{F}_1}(\omega) = \begin{cases} b & \text{if } \omega = \texttt{C/a} \\ c & \text{if } \omega = \texttt{B/b} \\ d & \text{if } \omega = \texttt{C/b} \\ a & \text{if } \omega \in \mathcal{L}_a \setminus \{\texttt{C/a}, \texttt{B/b}, \texttt{C/b}\} \\ \ell_\perp & \text{otherwise} \end{cases} \qquad \lambda_{\mathbb{F}_2}(\omega) = \begin{cases} d & \text{if } \omega = \texttt{C/b} \\ e & \text{if } \omega \in \mathcal{L}_e \setminus \{\texttt{C/b}\} \\ a & \text{if } \omega \in \mathcal{L}_a \setminus (\mathcal{L}_e \cup \{\texttt{C/b}\}) \\ \ell_\perp & \text{otherwise} \end{cases}$$

The graphs below in Figure 2 are pictorial representations of the concretisations of the Kripke models of the two configurations above (see Example 5).

Finally, the *CML* model of a pair of SEAndroid configurations can be computed by associating their Kripke models with the label evaluation obtained by inverting the file labelling function.

Definition 14 (*CML* Encoding). *The CML model of two SEAndroid configurations* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *is* $\{(\mathcal{K}_1, \downarrow_1), (\mathcal{K}_2, \downarrow_2)\}$*, where for* $i = 1, 2$*:* $\mathcal{K}_i$ *is the Kripke structure of* $\mathcal{C}_i$*;* $\downarrow_i \colon \mathbb{L}_{\mathtt{f}} \longrightarrow 2^{\Omega}$ *is such that* $\downarrow_i(\ell) = \{\omega \mid \lambda_{\mathbb{F}_i}(\omega) = \ell\}$ *for all* $\ell \in \mathbb{L}_{\mathtt{f}}$*, with* $\mathbb{F}_i$ *the file labeling policy of* $\mathcal{C}_i$*.*

We now use this encoding to compare two instances of SEAndroid in terms of their information flow through the procedure of Section 2.

Example 7. Consider the *CML* model for $\mathcal{C}_1$ and $\mathcal{C}_2$ of Figure 1. We start by computing the set of compatible worlds $\mathbb{S}$: a pair of file labels (ℓ, ℓ') is included in $\mathbb{S}$ if there exists at least a filepath that is associated with ℓ in the first policy and with ℓ' in the second one. For example, $(a, e) \in \mathbb{S}$ because of `A/a`, while $(c, e) \notin \mathbb{S}$ because c labels only `B/b` in $\mathbb{F}_1$ and e labels only filepaths ending with `a` in $\mathbb{F}_2$. Simple computations suffice for showing that $\mathbb{S} = \{[a, a], [a, e], [b, e], [c, a], [d, d]\}$. Consider the *CML* formula $\phi = \uparrow_1(\Diamond\texttt{untr}) \Rightarrow \uparrow_2(\texttt{usr} \wedge \Diamond\uparrow_1\texttt{untr})$. To check the validity of ϕ in our model, we take $\neg\phi$ and normalise it according to Definition 19 in the appendix. The result is $\psi = \uparrow_1\Diamond\uparrow_1\texttt{untr} \wedge (\neg\uparrow_2\texttt{usr} \vee \neg\uparrow_2\Diamond\uparrow_1\texttt{untr})$. We compute the compatible satisfaction set of ψ according to Definition 9: $[\![\psi]\!] = [\![\uparrow_1\Diamond\uparrow_1\texttt{untr}]\!] \setminus ([\![\uparrow_2\texttt{usr}]\!] \cup [\![\uparrow_2\Diamond\uparrow_1\texttt{untr}]\!]) = \{[b, e], [c, a]\} \setminus (\{[a, e], [b, e]\} \cup \{[a, e], [b, e]\}) = \{[c, a]\}$. The property is not satisfied, and concrete counterexamples are those files labelled as c in $\mathcal{C}_1$ and as a in $\mathcal{C}_2$, i.e. $\downarrow_1(c) \cap \downarrow_2(a) = \{\texttt{B/b}\}$.

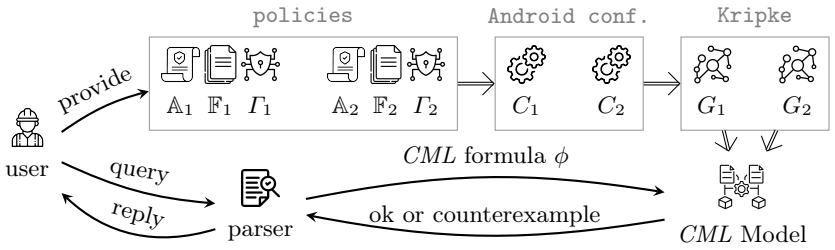


Fig. 5: Workflow of *Mordente*.

Algorithm 1 Compute the state evaluation $\downarrow_i$ of the i-th configuration.

Input: An ordered list $\mathbb{F}$ of pairs (ℓ, α) with ℓ a string and α an automaton
Output: A dictionary $\mathbb{D}$ from strings to automata

```
ζ ← L(ϵ)    D[ℓ] ← ∅ for all ℓ        ▷ ζ is the language of previously seen file paths
for all pairs (ℓ, α) in F do
    β ← α ∩ ζ^c                       ▷ ζ^c is the complement of ζ
    D[ℓ] ← D[ℓ] ∪ β
    ζ ← ζ ∪ β
return D
```

4 Implementation and Evaluation of *Mordente*

We implement our verification framework in the tool *Mordente*, available at [1]. Below, we discuss its internals and evaluate it on real-world policies.

***Mordente* Internals** The workflow of *Mordente* is in Figure 5. The user provides two compiled SEAndroid policies to be compared, each accompanied by its file context specification and its security policy Γ. For each policy, *Mordente* constructs a *SEAndroid configuration* $\mathcal{C} = (\mathbb{A}, \mathbb{F}, \Gamma)$ and then its *Kripke structure* $\mathcal{K}$. It then computes the *SEAndroid CML Model* for the pair of configurations, and waits for the user to submit CML queries for the differential verification.

More in detail, *Mordente* processes its input as follows. To build the access control policy $\mathbb{A}$, we extract all the *allow* rules from the compiled policy using setools [3]. Constructing the file labelling policy $\mathbb{F}$ requires additional work. We first process the file context entries in reverse order, as the Android system does. As a result, we obtain a list of pairs $(\texttt{regex}, \ell)$, where $\ell \in \mathbb{L}_{\texttt{f}}$ is a label and `regex` a regular expression of file paths. We then translate each `regex` into an equivalent finite state automaton using *libmata* [6]. To compute $\downarrow_i(\ell)$, the regular language of file paths associated with ℓ, we apply Algorithm 1, which iteratively refines each automaton to remove paths already matched by earlier entries, resolving shadowing between overlapping file context regexes. More precisely, Algorithm 1 returns a dictionary $\mathbb{D}$ from labels to automata, such that the language of $\mathbb{D}[\ell]$ is disjoint from the one of $\mathbb{D}[\ell']$ if $\ell \neq \ell'$. Note that if the

Algorithm 2 Approximate the relation $I \cap (\mathbb{L}_{\mathtt{f}} \times \mathbb{L}_{\mathtt{f}})$, preserving connectivity.

Input: A graph $G = (N, E)$
Output: G where all the nodes are file labels
1: **for all** $n \in N$ such that n is not a file label **do**
2: **for all** $(u, n) \in E$ with $u \neq n$ **do**
3: **for all** $(n, v) \in E$ with $n \neq v$ **do** ▷ u and v are connected
4: **if not** $(u, v) \in E$ **then** $E \leftarrow E \cup \{(u, v)\}$
5: Remove n from G
6: **return** G

Table 1: *Mordente* experimental evaluation.

(a) Generation of the Kripke models.

	file context lines	allow rules	build time (s)
① Pixel Comet (14)	1327	41296	436.24
② Pixel Comet (15)	1351	42744	454.74
③ Pixel Comet (16)	1397	45104	494.26
④ Xiaomi 11T	1940	52122	504.37
⑤ Xiaomi 14T	2264	63673	1188.80
⑥ Xiaomi 15T	2271	56784	1141.90

(b) Differential analysis.

	compatible states	build time (s)	query time (s)
① ↔ ②	769	17.52	2.18
② ↔ ③	814	17.51	2.39
① ↔ ④	1568	37.46	16.28
② ↔ ⑤	1592	38.11	13.96
② ↔ ⑥	1608	49.80	21.97

same label ℓ appears more than once in the file context, we take the union of the resulting automata. For efficiency, *Mordente* does not explicitly construct the full information flow relation I of Definition 11. Instead, it constructs a graph G whose nodes are SEAndroid labels and whose edges approximate I as follows: for each triple $(s, o, s') \in \mathbb{A}$, we add to G the edge (s, s') if $\triangleright \in \mathit{ife}(o)$ and (s', s) if $\triangleleft \in \mathit{ife}(o)$. The full information-flow relation I is then the transitive closure of G. We remove from G the non-file labels, i.e. those not in $\mathbb{D}$, while updating the edges to preserve connectivity: if two file labels were connected via a path possibly traversing non-file labels, the pruned graph maintains a path between them (see Algorithm 2). Then, the Kripke model $\mathcal{K}$ is obtained by considering the security policy Γ and associating atomic predicates to nodes of G accordingly.

After constructing both Kripke models, *Mordente* computes the set of compatible states of the *CML* Model: these are pairs of labels (ℓ_1, ℓ_2) such that the intersection of their corresponding automata recognises a non-empty language. Finally, once the user submits a *CML* formula ϕ, the verification proceeds as follows. We take $\neg\phi$ and compute its normal form $\psi^\bullet$ using the translation of Definition 19 in Appendix A. A custom model-checking procedure, based on Definition 9, computes the set of compatible states $[\![\psi^\bullet]\!]$ that falsify ϕ (note in passing that the modalities $\uparrow_i \Diamond$ and $\uparrow_i \blacklozenge$ are interpreted as reachability over the graph G). If $[\![\psi^\bullet]\!]$ is empty, the property ϕ holds; otherwise, a counterexample is generated by instantiating the offending states in $[\![\psi^\bullet]\!]$ with concrete file paths.

Experimental Evaluation We experimentally evaluated *Mordente* on a collection of policies from different vendors and Android versions. We automated the tests with a script, available at [1], which takes in input the Android firmware images of the systems to compare, it extracts the SEAndroid policy configuration files (precompiled policy, file contexts, and information about the Android version). The user can choose to perform either a *vertical* or an *horizontal* analysis. In the first case, policies are from the same vendor but from different Android versions, and are compared incrementally, each version with the next one; in the second case, the policies are from different vendors (presumably of the same Android version) and are compared in every possible combination. During the analysis, *Mordente* is first invoked once for each SEAndroid configuration to compute its Kripke structure, which is then saved for future use. Then, the tool is applied to each pair of policies to compute their *CML* Model and compatible states, and finally to check the validity of the submitted queries.

We evaluated *Mordente* on 6 configurations as reported in Table 1: three are from major Android releases (14, 15, 16) of the firmware for a Pixel 9 Pro Fold (*Comet*) [8]; three others are from different Xiaomi devices (11T, 14T, 15T) [18], selected with a similar Android version (14, 15). The experiments were conducted on a virtual machine with 4 cores of an Intel Core i7-10700 K processor (3.80 GHz) and 16GB of RAM, running Ubuntu 24.04. In more detail, Table 1a shows the size of each considered configuration (the number of file context lines and *allow* rules) as well as the time it takes on average over 10 executions to construct its Kripke structure. We analysed Pixel configurations vertically (comparing each version with the next one); whereas each Xiaomi configuration was assessed against the same Android major version of Pixel. Table 1b reports the results of our differential analysis over the selected pairs of configurations: the number of compatible states, the time to compute the resulting *CML* model, and the time to verify 7 formulas discussed in Appendix B (average over 10 executions).

Overall, the time needed to compute the Kripke structure is acceptable for both vendors. Furthermore, the time required to compute a *CML* model is considerably smaller, and the queries are almost instant. In addition, *Mordente* is capable of storing the computed Kripke structure and reload it when needed, vastly reducing the expected loading times by a factor of 20 on average.

5 Related Work

The security of SEAndroid and SELinux has been extensively studied in the literature from various perspectives. Below, we first discuss proposals that examine how SEAndroid policies have evolved over the years and across various vendors. Then, we consider research on verifying information-flow properties in SELinux.

Im et al. [11] perform a historical analysis on the AOSP repository to understand the evolution of SEAndroid policy. In particular, the authors propose a metric for the complexity of policies and measure different commits of the main branch of the repository: the complexity of SEAndroid policies has been growing exponentially over time, confirming the necessity of specialised tools and

techniques for their analysis. Yu et al. [19] investigate the status of SEAndroid policy customisation, namely, the differences in terms of permissions between the official AOSP policy and the versions of vendors. They propose the tool SEPAL to automatically predict whether the customised policy rules are potentially risky or unnecessary, using natural language processing techniques. Posemato et al. [14] perform a longitudinal study on Android OEM customisations with the goal of determining if these customisations lead to compatibility and security problems. They consider the various requirements imposed by Google to brand a device "Android", including some over SEAndroid. They highlighted that many customisations removed some `neverallow` rules from the AOSP policy, weakening the security of the resulting policy. The papers above compare SEAndroid policies using ad hoc algorithms that analyse individual rules and their granted permissions. In contrast, our work assigns a formal semantics to SEAndroid policies and verifies them not at the level of single rules, but in terms of the information flows induced by the permissions collectively granted across multiple rules. Moreover, our logic and model-checking procedure enable policy analysts to express and verify a variety of relational queries over pairs of policies, offering greater expressiveness than rule-by-rule comparison.

Some tools have been proposed to compare two SELinux policies. The `sediff` tool [16] is a command-line utility, part of the SETools (SELinux Policy Analysis Tools) suite, used to compare and find the semantic differences between two SELinux policies. The tool operates at the entity level and highlights differences in various policy elements, including rules, types, and attributes. More precisely, given two policies, the tool can detect if an element exists only in one of the two policies or if it has been modified, namely, it exists in both policies, but the associated permissions have changed. The V3SPA [9] is a visualisation tool for SELinux policies that supports policy analysts in understanding the meaning of a policy and performing differential policy analysis, highlighting the changes between two policy versions. Policies are depicted as graphs, where nodes represent subjects and objects, and edges represent the permissions associated with them. These graphs can be manually inspected by analysts. These tools offer limited analysis capabilities because they either focus on individual permissions or require policy analysts to manually compare graph representations of the policies. In contrast, our approach supports the specification of more expressive information-flow properties and automatically checks them, thereby providing better scalability and generality. In addition, our work is the first to compare permissions in terms of concrete files, considering possibly different labelling policies, whereas previous approaches only reason at the level of labels.

Several papers target information flow in SELinux policies. Radika et. al. [15] analyse SELinux configurations to identify potentially dangerous information flows, defined by the authors as those from some entity a to some b such that a `neverallow` rule prohibits a direct read access from b to a. They developed a tool to statically investigate such information flows, and applied it to the AOSP policy; Jaeger et al. [12] analyse the SELinux example policy for Linux 2.4.19, identifying the trusted computing base and studying its integrity. Hernandez et al. [10]

investigate the Android policy environment, including SEAndroid, UNIX-style DAC, and Linux capabilities, and propose BigMAC, a framework that unifies all policy layers to produce a large, fine-grained attack graph. A logic-based query engine is then used to prune infeasible paths and unused types. Similarly, Lee et al. [13] describe PolyScope, a tool for analysing Android systems and identifying resources that attackers can modify, with and without policy manipulations. For each integrity violation detected, PolyScope characterises how attacks may be mounted. Ceragioli et al. [5] enriched the intermediate language CIL, used to specify SELinux configurations with a formal semantics and mechanisms to allow users to specify and verify information-flow requirements. All these papers analyse one policy at a time and therefore cannot detect differences in permitted information flow across different policies. In contrast, our proposal enables the specification and verification of information-flow properties over pairs of policies, thus supporting change-impact analysis of SEAndroid configurations.

6 Conclusion

We have presented a differential verification framework for SEAndroid that enables reasoning across multiple versions or vendor variants of a policy, capturing how changes in the permissions and labelling affect the information-flow properties. Our framework is built on *CML*, a modal logic that we designed explicitly to express comparative properties across pairs of Kripke structures. We have formalised SEAndroid policies as Kripke structures and have defined a suitable *CML* model-checking algorithm for differential reasoning on them. We have implemented our approach in the *Mordente* tool and evaluated its scalability on real-world SEAndroid policies from different vendors and Android releases. Our experiments show that differential verification is feasible in practice. To the best of our knowledge, *Mordente* is the first tool to compare SEAndroid configurations in a formally grounded way that simultaneously accounts for changes in both the permission and labelling policies. A key advantage of *Mordente* is that it allows proving the preservation of undocumented security properties.

Future work includes using *Mordente* to perform a large-scale security analysis of SEAndroid customisation to identify security-relevant deviations. Moreover, we plan to extend *Mordente* by integrating automated repair strategies for policy regressions.

References

1. Mordente: Tool for Differential Verification of Information Flow in SEAndroid Policies, https://github.com/edoxthebest/Mordente
2. Selinux project. https://selinuxproject.org
3. Setools: Policy analysis tools for selinux. https://github.com/SELinuxProject/setools
4. The SELinux Notebook - Kernel Policy Language. https://github.com/SELinuxProject/selinux-notebook/blob/main/src/kernel_policy_language.md#kernel-policy-language

5. Ceragioli, L., Galletta, L., Degano, P., Basin, D.: Specifying and verifying information flow control in selinux configurations. ACM Trans. Priv. Secur. **27**(4) (2024)
6. Chocholatý, D., Fiedor, T., Havlena, V., Holík, L., Hruška, M., Lengál, O., Síč, J.: Mata: A fast and simple finite automata library. In: Finkbeiner, B., Kovács, L. (eds.) Tools and Algorithms for the Construction and Analysis of Systems. pp. 130–151. Springer Nature Switzerland, Cham (2024)
7. Drake, J.: Stagefright: Scary Code in the Heart of Android (2015), https://blackhat.com/docs/us-15/materials/us-15-Drake-Stagefright-Scary-Code-In-The-Heart-Of-Android.pdf, BlackHat USA
8. Google: Full ota images for nexus and pixel devices. https://developers.google.com/android/ota
9. Gove, R.: V3spa: A visual analysis, exploration, and diffing tool for selinux and seandroid security policies. In: 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). pp. 1–8 (2016). https://doi.org/10.1109/VIZSEC.2016.7739580
10. Hernandez, G., Tian, D.J., Yadav, A.S., Williams, B.J., Butler, K.R.: BigMAC: Fine-Grained policy analysis of Android firmware. In: 29th USENIX Security Symposium (USENIX Security 20). pp. 271–287. USENIX Association (Aug 2020), https://www.usenix.org/conference/usenixsecurity20/presentation/hernandez
11. Im, B., Chen, A., Wallach, D.S.: An historical analysis of the seandroid policy evolution. In: Proceedings of the 34th Annual Computer Security Applications Conference. p. 629–640. ACSAC '18, Association for Computing Machinery, New York, NY, USA (2018). https://doi.org/10.1145/3274694.3274709, https://doi.org/10.1145/3274694.3274709
12. Jaeger, T., Sailer, R., Zhang, X.: Analyzing integrity protection in the selinux example policy. In: Procs 12th USENIX Security Symposium, Washington, D.C., USA, 2003. USENIX Association (2003)
13. Lee, Y.T., Enck, W., Chen, H., Vijayakumar, H., Li, N., Qian, Z., Wang, D., Petracca, G., Jaeger, T.: PolyScope: Multi-Policy access control analysis to compute authorized attack operations in Android systems. In: 30th USENIX Security Symposium (USENIX Security 21). pp. 2579–2596. USENIX Association (Aug 2021), https://www.usenix.org/conference/usenixsecurity21/presentation/lee-yu-tsung
14. Possemato, A., Aonzo, S., Balzarotti, D., Fratantonio, Y.: Trust, but verify: A longitudinal analysis of android oem compliance and customization. In: 2021 IEEE Symposium on Security and Privacy (SP). pp. 87–102 (2021). https://doi.org/10.1109/SP40001.2021.00074
15. Radhika, B.S., Kumar, N.V.N., Shyamasundar, R.K., Vyas, P.: Consistency analysis and flow secure enforcement of selinux policies. Comput. Secur. **94**, 101816 (2020)
16. SETools: Policy analysis tools for SELinux, https://github.com/SELinuxProject/setools
17. Seri, B., Vishnepolsky, G.: The dangers of bluetooth implementations: Unveiling zero day vulnerabilities and security flaws in modern bluetooth stacks. Tech. rep., Armis INC. White Paper (2023), https://info.armis.com/rs/645-PDC-047/images/BlueBorne%20Technical%20White%20Paper_20171130.pdf
18. Xiaomi: Xiaomi community. https://c.mi.com/global/miuidownload/index
19. Yu, D., Yang, G., Meng, G., Gong, X., Zhang, X., Xiang, X., Wang, X., Jiang, Y., Chen, K., Zou, W., Lee, W., Shi, W.: Sepal: Towards a large-scale analysis of seandroid policy customization. In: Proceedings of the Web Conference 2021. p. 2733–2744. WWW '21, Association for Computing Machinery, New York, NY,

USA (2021). https://doi.org/10.1145/3442381.3450007, https://doi.org/10.1145/3442381.3450007

A Proofs

Lemma 1. *For each CML proposition in normal form ϕ, concrete state $\omega \in \Omega$ and model $\mathcal{M}$, if $\omega, i \models_{\mathcal{M}} \phi$ for some i, then it holds that $\omega \models_{\mathcal{M}} \phi$.*

Proof. A simple induction over the semantics of $\Phi^\bullet$ suffices.

Definition 15 (Equivalence of *CML* Formulas). *Two CML formulas ϕ and ψ are equivalent ($\phi \equiv \psi$) whenever for any CML model $\mathcal{M}$*

$$\omega \models_{\mathcal{M}} \phi \text{ if and only if } \omega \models_{\mathcal{M}} \psi.$$

Definition 16 (Positive Form). *CML propositions in* positive form *are generated by the following grammar, with $i \in \mathbb{I}$ a version and $p \in \mathbb{P}$ atomic proposition.*

$$\phi ::= \mathit{true} \mid \mathit{false} \mid p \mid \neg p \mid \phi \wedge \phi \mid \phi \vee \phi \mid \uparrow_i \phi \mid \Diamond \phi \mid \blacklozenge \phi \mid \Box \phi \mid \blacksquare \phi$$

We let $\Phi^\circ \subsetneq \Phi$ be the set of CML propositions in positive form.

Definition 17 (*CML* Positive Translation). *We let the CML* normalizing translation $\_^\circ : \Phi \to \Phi^\circ$ *be defined as follows:*

$$\begin{aligned}
\mathit{true}^\circ &= \mathit{true} & \neg\mathit{true}^\circ &= \mathit{false} \\
(\phi \wedge \psi)^\circ &= \phi^\circ \wedge \psi^\circ & (\neg(\phi \wedge \psi))^\circ &= (\neg\phi)^\circ \vee (\neg\psi)^\circ \\
(\uparrow_i \phi)^\circ &= \uparrow_i (\phi^\circ) & (\neg\uparrow_i \phi)^\circ &= \uparrow_i ((\neg\phi)^\circ) \\
(\Diamond\phi)^\circ &= \Diamond(\phi^\circ) & (\neg\Diamond\phi)^\circ &= \Box((\neg\phi)^\circ) \\
(\blacklozenge\phi)^\circ &= \blacklozenge(\phi^\circ) & (\neg\blacklozenge\phi)^\circ &= \blacksquare((\neg\phi)^\circ) \\
p^\circ &= p & (\neg p)^\circ &= \neg p
\end{aligned}$$

Lemma 2. *The CML positive translation of Definition 17 terminates and is such that $\phi \equiv \phi^\circ$.*

Proof. For termination is suffices noticing that computing ϕ° requires computing ψ° only if ψ is smaller then ϕ. Correctness is proved by induction on the translation function. □

Definition 18 (*CML* Positive Normalizing Translation). *We let the CML* positive normalizing translation $\_^\star : \Phi^\circ \to \Phi^\bullet$ *be defined as follows:*

$$
\begin{aligned}
true^\bullet &= true \\
false^\bullet &= false \\
(\phi \wedge \psi)^\bullet &= \phi^\bullet \wedge \psi^\bullet \\
(\phi \vee \psi)^\bullet &= \phi^\bullet \vee \psi^\bullet \\
(\Diamond\phi)^\bullet &= \bigwedge_{i\in\mathbb{I}} \uparrow_i \Diamond(\uparrow_i \phi)^\bullet \\
(\blacklozenge\phi)^\bullet &= \bigwedge_{i\in\mathbb{I}} \uparrow_i \blacklozenge(\uparrow_i \phi)^\bullet \\
(\Box\phi)^\bullet &= \bigwedge_{i\in\mathbb{I}} \uparrow_i \Box(\uparrow_i \phi)^\bullet \\
(\blacksquare\phi)^\bullet &= \bigwedge_{i\in\mathbb{I}} \uparrow_i \blacksquare(\uparrow_i \phi)^\bullet \\
p^\bullet &= \bigwedge_{i\in\mathbb{I}} \uparrow_i p \\
(\neg p)^\bullet &= \bigwedge_{i\in\mathbb{I}} \uparrow_i \neg p
\end{aligned}
\qquad
\begin{aligned}
(\uparrow_i true)^\bullet &= true \\
(\uparrow_i false)^\bullet &= false \\
(\uparrow_i(\phi \wedge \psi))^\bullet &= (\uparrow_i \phi)^\bullet \wedge (\uparrow_i \psi)^\bullet \\
(\uparrow_i(\phi \vee \psi))^\bullet &= (\uparrow_i \phi)^\bullet \vee (\uparrow_i \psi)^\bullet \\
(\uparrow_i \Diamond\phi)^\bullet &= \uparrow_i \Diamond(\uparrow_i \phi)^\bullet \\
(\uparrow_i \blacklozenge\phi)^\bullet &= \uparrow_i \blacklozenge(\uparrow_i \phi)^\bullet \\
(\uparrow_i \Box\phi)^\bullet &= \uparrow_i \Box(\uparrow_i \phi)^\bullet \\
(\uparrow_i \blacksquare\phi)^\bullet &= \uparrow_i \blacksquare(\uparrow_i \phi)^\bullet \\
(\uparrow_i p)^\bullet &= \uparrow_i p \\
(\uparrow_i \neg p)^\bullet &= \neg\uparrow_i p \\
(\uparrow_i \uparrow_j \phi)^\bullet &= (\uparrow_j \phi)^\bullet
\end{aligned}
$$

Lemma 3. *The CML positive normalizing translation terminates.*

Proof. Note that $\phi^\bullet$ is defined in terms of $\psi^\bullet$ only if one of the following conditions holds:

- ψ has strictly fewer occurrences of *CML* operators than ϕ;
- ψ has the exact same amount of occurrences of *CML* operators than ϕ, but strictly fewer of them differ from $\uparrow_i$ for any i.

Let α_ϕ be the number of occurrences of *CML* operators in ϕ, and β_ϕ the number of occurrences of *CML* operators in ϕ that differ from $\uparrow_i$ for any i *CML*. Then $\alpha_\phi\beta_\phi$ recursive calls suffice to compute $\phi^\bullet$ in the worst case. □

Lemma 4. *The CML positive normalizing translation is such that* $\phi \equiv \phi^\bullet$.

Proof. We proceed by induction over the definition of the $\_^\bullet$ function, i.e. for each rule of its definition we show that assuming $\phi \equiv \phi^\bullet$ for all the ϕ occurring in the body of the rule suffices for showing that $\psi \equiv \psi^\bullet$ with ψ the argument of the translation in the head of the rule.

(case *true*, *false*, $\uparrow_i p$, $\uparrow_i \neg p$**)**
Trivially holds by definition.

(case $\uparrow_i true$**)**

$$
\begin{aligned}
\omega \models \uparrow_i true \text{ iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, j \models \uparrow_i true \\
\text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, i \models true \\
\text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, j \models true \\
\text{iff } \omega \models true \text{ iff } \omega \models (\uparrow_i true)^\bullet
\end{aligned}
$$

(case $\uparrow_i \mathit{false}$)
Follows the same schema as (case $\uparrow_i \mathit{true}$).

(case $(\phi \wedge \psi)$)
Assume $\phi^\bullet \equiv \phi$ and $\psi^\bullet \equiv \psi$, then

$$\begin{aligned}
\omega \models \phi \wedge \psi \text{ iff } & \text{for all } i \in \mathbb{I}, \text{ it holds that } \omega, i \models \phi \wedge \psi \\
& \text{iff for all } i \in \mathbb{I}, \text{ it holds that } \omega, i \models \phi \text{ and } \omega, i \models \psi \\
& \text{iff for all } i \in \mathbb{I}, \text{ it holds that } \omega, i \models \phi^\bullet \text{ and } \omega, i \models \psi^\bullet \\
& \text{iff for all } i \in \mathbb{I}, \text{ it holds that } \omega, i \models \phi^\bullet \wedge \psi^\bullet \\
& \text{iff } \omega \models \phi^\bullet \wedge \psi^\bullet \text{ iff } \omega \models (\phi \wedge \psi)^\bullet
\end{aligned}$$

(case $(\phi \vee \psi)$)
Works as (case $(\phi \wedge \psi)$)

(case $\uparrow_i(\phi \wedge \psi)$)
Assume $(\uparrow_i \phi)^\bullet \equiv (\uparrow_i \phi)$ and $(\uparrow_i \psi)^\bullet \equiv (\uparrow_i \psi)$, then

$$\begin{aligned}
\omega \models \uparrow_i(\phi \wedge \psi) \text{ iff } & \text{for all } j \in \mathbb{I}, \text{ it holds that } \omega, j \models \uparrow_i(\phi \wedge \psi) \\
& \text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, i \models \phi \wedge \psi \\
& \text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, i \models \phi \text{ and } \omega, i \models \psi \\
& \text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, j \models \uparrow_i \phi \text{ and } \omega, j \models \uparrow_i \psi \\
& \text{iff } \omega \models \uparrow_i \phi \text{ and } \omega \models \uparrow_i \psi \\
& \text{iff } \omega \models (\uparrow_i \phi)^\bullet \text{ and } \omega \models (\uparrow_i \psi)^\bullet \\
& \text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, j \models (\uparrow_i \phi)^\bullet \text{ and } \omega, j \models (\uparrow_i \psi)^\bullet \\
& \text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, j \models (\uparrow_i \phi)^\bullet \wedge (\uparrow_i \psi)^\bullet \\
& \text{iff } \omega \models (\uparrow_i \phi)^\bullet \wedge (\uparrow_i \phi)^\bullet \text{ iff } \omega \models (\uparrow_i (\phi \wedge \phi))^\bullet
\end{aligned}$$

(case $\uparrow_i(\phi \vee \psi)$)
Works as (case $\uparrow_i(\phi \wedge \psi)$).

(case $\uparrow_i \Diamond \phi$)
Assume $(\uparrow_i \phi)^\bullet \equiv \uparrow_i \phi$, then

$$\begin{aligned}
\omega \models \uparrow_i \Diamond \phi \text{ iff } & \omega, i \models \Diamond \phi \\
& \text{iff } \omega' \text{ exists with } \omega \mapsto\!\!\blacktriangleright_i \omega' \text{ and } \omega', i \models \phi \\
& \text{iff for all } j \in \mathbb{I}, \omega' \text{ exists with } \omega \mapsto\!\!\blacktriangleright_i \omega' \text{ and } \omega', j \models \uparrow_i \phi \\
& \text{iff for all } j \in \mathbb{I}, \omega' \text{ exists with } \omega \mapsto\!\!\blacktriangleright_i \omega' \text{ and } \omega', j \models (\uparrow_i \phi)^\bullet \\
& \text{iff } \omega, i \models \Diamond (\uparrow_i \phi)^\bullet \\
& \text{iff for all } j \in \mathbb{I}, \text{ it holds that } \omega, j \models \uparrow_i \Diamond (\uparrow_i \phi)^\bullet \\
& \text{iff } \omega \models \uparrow_i \Diamond (\uparrow_i \phi)^\bullet \text{ iff } \omega \models (\uparrow_i \Diamond \phi)^\bullet
\end{aligned}$$

(case $\uparrow_i \Box \phi$)

Assume $(\uparrow_i \phi)^\bullet \equiv \uparrow_i \phi$, then

$\omega \models \uparrow_i \Box \phi$ iff $\omega, i \models \Box \phi$
iff for all ω' with $\omega \mapsto\!\!\blacktriangleright_i \omega'$ it holds $\omega', i \models \phi$
iff for all $j \in \mathbb{I}$, ω' s.t. $\omega \mapsto\!\!\blacktriangleright_i \omega'$ it holds $\omega', j \models \uparrow_i \phi$
iff for all $j \in \mathbb{I}$, ω' s.t. $\omega \mapsto\!\!\blacktriangleright_i \omega'$ it holds $\omega', j \models (\uparrow_i \phi)^\bullet$
iff $\omega, i \models \Box(\uparrow_i \phi)^\bullet$
iff for all $j \in \mathbb{I}$, it holds that $\omega, j \models \uparrow_i \Box(\uparrow_i \phi)^\bullet$
iff $\omega \models \uparrow_i \Box(\uparrow_i \phi)^\bullet$ iff $\omega \models (\uparrow_i \Box \phi)^\bullet$

(case p)

$\omega \models p$ iff for all $i \in \mathbb{I}$, it holds that $\omega, i \models p$
iff for all $i, j \in \mathbb{I}$, it holds that $\omega, i \models \uparrow_j p$
iff for all $j \in \mathbb{I}$, it holds that $\omega, j \models \bigwedge_{i \in \mathbb{I}} \uparrow_i p$
iff $\omega \models \bigwedge_{i \in \mathbb{I}} \uparrow_i p$ iff $\omega \models p^\bullet$

(case $\neg p$)

Works as (case p).

(case $\Diamond \phi$)

Assume $(\uparrow_i \phi)^\bullet \equiv \uparrow_i \phi$, then

$\omega \models \Diamond \phi$ iff for all $i \in \mathbb{I}$, it holds that $\omega, i \models \Diamond \phi$
iff for all $i \in \mathbb{I}$, it holds that ω' exists with $\omega \mapsto\!\!\blacktriangleright_i \omega'$ and $\omega', i \models \phi$
iff for all $i, j \in \mathbb{I}$, it holds that ω' exists with $\omega \mapsto\!\!\blacktriangleright_i \omega'$ and $\omega', j \models \uparrow_i \phi$
iff for all $i, j \in \mathbb{I}$, it holds that ω' exists with $\omega \mapsto\!\!\blacktriangleright_i \omega'$ and $\omega', j \models (\uparrow_i \phi)^\bullet$
iff for all $i, j \in \mathbb{I}$, it holds that $\omega, j \models \uparrow_i \Diamond (\uparrow_i \phi)^\bullet$
iff for all $j \in \mathbb{I}$, it holds that $\omega, j \models \bigwedge_{i \in \mathbb{I}} \uparrow_i \Diamond (\uparrow_i \phi)^\bullet$
iff $\omega \models \bigwedge_{i \in \mathbb{I}} \uparrow_i \Diamond (\uparrow_i \phi)^\bullet$ iff $\omega \models (\Diamond \phi)^\bullet$

(case $\Box \phi$)

Assume $(\uparrow_i \phi)^\bullet \equiv \uparrow_i \phi$, then

$\omega \models \Box\phi$ iff for all $i \in \mathbb{I}$, it holds that $\omega, i \models \Box\phi$
iff for all $i \in \mathbb{I}$, ω' s.t. $\omega \mapsto\!\!\blacktriangleright_i \omega'$, it holds that $\omega', i \models \phi$
iff for all $i, j \in \mathbb{I}$, ω' s.t. $\omega \mapsto\!\!\blacktriangleright_i \omega'$ it holds that $\omega', j \models \uparrow_i \phi$
iff for all $i, j \in \mathbb{I}$, it holds that for all ω' with $\omega \mapsto\!\!\blacktriangleright_i \omega'$ it holds that $\omega', j \models (\uparrow_i \phi)^\bullet$
iff for all $i, j \in \mathbb{I}$, it holds that $\omega, j \models \uparrow_i \Box(\uparrow_i \phi)^\bullet$
iff for all $j \in \mathbb{I}$, it holds that $\omega, j \models \bigwedge_{i \in \mathbb{I}} \uparrow_i \Box(\uparrow_i \phi)^\bullet$
iff $\omega \models \bigwedge_{i \in \mathbb{I}} \uparrow_i \Box(\uparrow_i \phi)^\bullet$ iff $\omega \models (\Box\phi)^\bullet$

(case $\uparrow_i \blacklozenge \phi$)
The proof is the same of (case $\uparrow_i \Diamond \phi$), with $\omega' \mapsto\!\!\blacktriangleright_i \omega$ in place of $\omega \mapsto\!\!\blacktriangleright_i \omega'$.
(case $\uparrow_i \blacksquare \phi$)
The proof is the same of (case $\uparrow_i \Box \phi$), with $\omega' \mapsto\!\!\blacktriangleright_i \omega$ in place of $\omega \mapsto\!\!\blacktriangleright_i \omega'$.
(case $\blacklozenge \phi$)
The proof is the same of (case $\Diamond \phi$), with $\omega' \mapsto\!\!\blacktriangleright_i \omega$ in place of $\omega \mapsto\!\!\blacktriangleright_i \omega'$.
(case $\blacksquare \phi$)
The proof is the same of (case $\Box \phi$), with $\omega' \mapsto\!\!\blacktriangleright_i \omega$ in place of $\omega \mapsto\!\!\blacktriangleright_i \omega'$.
(case $\uparrow_i \uparrow_j \phi$)
Assume $(\uparrow_j \phi)^\bullet \equiv \uparrow_j \phi$, then

$\omega \models \uparrow_i \uparrow_j \phi$ iff $\omega, i \models \uparrow_j \phi$
iff $\omega, j \models \phi$
iff for all $k \in \mathbb{I}$, it holds that $\omega, k \models \uparrow_j \phi$
iff $\omega \models \uparrow_j \phi$ iff $\omega \models (\uparrow_i \uparrow_j \phi)^\bullet$

□

Definition 19 (*CML* Normalizing Translation). *We let the CML* normalizing translation $\_^\bullet \colon \Phi \to \Phi^\bullet$ *be defined as the composition of* $\_^\star$ *and* $\_^\circ$.

Theorem 1. *For each CML proposition ϕ, there exists a CML proposition in normal form $\phi^\bullet$ such that $\omega \models_{\mathcal{M}} \phi$ if and only if $\omega \models_{\mathcal{M}} \phi^\bullet$ for any ω and $\mathcal{M}$.*

Proof. Using the normalizing translation of Definition 19 suffices, and its correctness derives from Lemmas 2 to 4.

□

Definition 20 (Compatible State Evaluation). *Given a CML model $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i \in \mathbb{I}}$ and its set of compatible states $\mathbb{S} \subseteq \prod_{i \in \mathbb{I}} S_i$, we write $\Downarrow \colon \mathbb{S} \longrightarrow 2^\Omega$ for the* compatible state evaluation *of $\mathcal{M}$ associating $\bar{s}$ with $\bigcap_{i \in \mathbb{I}} \downarrow_i (\bar{s}[i])$.*

Lemma 5. *Given a CML model $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i \in \mathbb{I}}$, its set of compatible states $\mathbb{S}$, and its compatible state evaluation $\Downarrow \colon \mathbb{S} \longrightarrow 2^\Omega$, it holds that $\bigcup_{\bar{s} \in \mathbb{S}} \Downarrow \bar{s} = \Omega$.*

Proof. Take any $\omega \in \Omega$, then, by Definition 3, some s_i exist for each i such that $\omega \in \downarrow_i(s_i)$. Let $\bar{s}$ be such that $\bar{s}[i] = s_i$ as defined above, then $\omega \in \Downarrow \bar{s}$ by construction. □

Lemma 6. *Given a CML model $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i\in\mathbb{I}}$, its set of compatible states $\mathbb{S}$, and its compatible state evaluation $\Downarrow\colon \mathbb{S} \longrightarrow 2^{\Omega}$, if $\bar{s}[i] \neq \bar{s}'[i]$ for some $i \in \mathbb{I}$, then $\Downarrow(\bar{s}) \cap \Downarrow(\bar{s}') = \emptyset$.*

Proof. Assume by refutation that $s = \bar{s}[i] \neq \bar{s}'[i] = s' \in S_i$ and ω exists with $\omega \in \Downarrow(\bar{s}) \cap \Downarrow(\bar{s}')$. Then $\omega \in \downarrow_i(\bar{s}[i]) \cap \downarrow_i(\bar{s}'[i]) = \downarrow_i(s) \cap \downarrow_i(s')$, but by Definition 3 the latter is empty. □

Lemma 7. *Given a CML model $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i\in\mathbb{I}}$, its set of compatible states $\mathbb{S}$, and its compatible state evaluation $\Downarrow\colon \mathbb{S} \longrightarrow 2^{\Omega}$, for all $i \in \mathbb{I}$ and $\omega \in \Omega$, if $\omega \in \downarrow_i(s)$ for some $s \in S_i$, then $\omega \in \Downarrow(\bar{s})$ for some $\bar{s} \in \mathbb{S}$ such that $\bar{s}[i] = s$.*

Proof. Assume $\omega \in \downarrow_i(s)$ for some $s \in S_i$. Then, by Definition 3, some s_j exists for any $j \in \mathbb{I}$ such that $\omega \in \downarrow_j(s_j)$. Therefore, we take $\bar{s}$ such that $\bar{s}[i] = s$ and $\bar{s}[j] = s_j$ for any $j \neq i$. Finally, $\omega \in \Downarrow(\bar{s})$ holds by construction. □

Theorem 2. *Given a CML model $\mathcal{M} = \{(\mathcal{K}_i, \downarrow_i)\}_{i\in I}$, it holds for all $\omega \in \Omega$ and $\phi \in \Phi^{\bullet}$ that $\omega \models_{\mathcal{M}} \phi$ if and only if $\omega \in \bigcup_{\bar{s}\in[\![\phi]\!]} \bigcap_{i\in I} \downarrow_i \bar{s}[i]$*

Proof. We assume $\mathcal{K}_i = (S_i, \rightarrowtriangle_i, \vdash_i)$, with $(\Omega, \mapsto_i, \Vdash_i)$ its concretization with respect to $\downarrow_i$. We let $\mathbb{S}$ to be the set of compatible states of $\mathcal{M}$, and $\Downarrow$ its compatible state evaluation.

We prove $\omega \models \phi$ iff $\omega \in \bigcup_{\bar{s}\in[\![\phi]\!]} \Downarrow(\bar{s})$ by induction on the syntax of *CML* propositions in normal form. Notice that in the following we apply Lemma 1 extensively without recalling it.

(case *true***)**

Note that $\omega \models \mathit{true}$ holds by definition.

For the converse, since $[\![\mathit{true}]\!] = \mathbb{S}$, we have to prove that for each ω, some $\bar{s} \in \mathbb{S}$ exists such that $\omega \in \Downarrow(\bar{s})$, which derives from Lemma 5.

(case $\uparrow_i p$)

We have that $[\![\uparrow_i p]\!] = \{\bar{s} \in \mathbb{S} \mid \bar{s}[i] \vdash_i p\}$

Assume $\omega \models \uparrow_i p$, and thus $\omega \Vdash_i p$. By Definition 4, $\omega \in \downarrow_i(s)$ for some $s \in S_i$ such that $s \vdash_i p$. Therefore, by Lemma 7, $\omega \in \Downarrow(\bar{s})$ for some $\bar{s}$ with $\bar{s}[i] = s$. Finally, note that $\bar{s} \in [\![\uparrow_i p]\!]$ by definition.

For the converse, assume $\omega \in \Downarrow(\bar{s})$ for some $\bar{s} \in [\![\uparrow_i p]\!]$. Then $\bar{s}[i] \vdash_i p$ by definition, and since $\omega \in \Downarrow(\bar{s})$ implies $\omega \in \downarrow_i(\bar{s}[i])$, $\omega \Vdash_i p$ by Definition 4, and thus $\omega \models \uparrow_i p$.

(case $\phi \wedge \phi'$)

We have that $[\![\phi \wedge \phi']\!] = [\![\phi]\!] \cap [\![\phi']\!]$.

Assume $\omega \models \phi \wedge \phi'$, and hence $\omega \models \phi$ and $\omega \models \phi'$. Then, by induction hypothesis, $\omega \in \Downarrow(\bar{s})$ for some $\bar{s} \in [\![\phi]\!]$, and $\omega \in \Downarrow(\bar{s}')$ for some $\bar{s}' \in [\![\phi']\!]$. But then, since $\omega \in \Downarrow(\bar{s}) \cap \Downarrow(\bar{s}')$, it must be that $\bar{s}[i] = \bar{s}'[i]$ for all $i \in \mathbb{I}$ by Lemma 6. Thus, $\omega \in \Downarrow(\bar{s})$ for $\bar{s} \in [\![\phi]\!] \cap [\![\phi']\!]$.

For the converse, assume $\omega \in \Downarrow(\bar{s})$ for some $\bar{s} \in [\![\phi \wedge \phi']\!]$. Then $\bar{s} \in [\![\phi]\!]$ and $\bar{s} \in [\![\phi']\!]$, and by induction hypothesis it holds that $\omega \models \phi$ and $\omega \models \phi'$.

(case $\neg\phi$)

We have that $[\![\neg\phi]\!] = \mathbb{S} \setminus [\![\phi]\!]$.

Assume $\omega \models \neg\phi$, and thus $\omega \not\models \phi$. Note that, by Lemma 5, a state $\bar{s} \in \mathbb{S}$ must exist such that $\omega \in \Downarrow(\bar{s})$. Moreover, $\bar{s} \notin [\![\phi]\!]$ because by induction hypothesis, $\bar{s} \in [\![\phi]\!]$ would imply $\omega \models \phi$.

For the converse, assume $\omega \in \Downarrow(\bar{s})$ for some $\bar{s} \in [\![\neg\phi]\!]$. Then, by Lemma 6 it holds that for all $\bar{s}' \in [\![\phi]\!]$, $\omega \notin \Downarrow(\bar{s}')$, and thus $\omega \not\models \phi$.

(case $\uparrow_i \Diamond\phi$)

We have that

$$[\![\uparrow_i \Diamond\phi]\!] = \{\bar{s} \mid \bar{s}' \in [\![\phi]\!] \text{ exists such that } \bar{s}[i] \longrightarrow_i \bar{s}'[i]\}$$

Assume $\omega \models \uparrow_i \Diamond\phi$, and thus $\omega \mapsto_i \omega'$ for some ω' such that $\omega' \models \phi$. By Definition 4, $\omega \mapsto_i \omega'$ implies that $s, s' \in S_i$ exist such that $s \longrightarrow_i s'$, with $\omega \in \downarrow_i(s)$ and $\omega' \in \downarrow_i(s')$. By Lemma 7, $\bar{s}$ and $\bar{s}'$ exist in $\mathbb{S}$ with $\bar{s}[i] = s \longrightarrow_i s' = \bar{s}'[i]$ and such that $\omega \in \Downarrow \bar{s}$ and $\omega' \in \Downarrow \bar{s}'$. Moreover, by induction hypothesis, $\omega' \models \phi$ implies that $\omega' \in \Downarrow(\bar{s}'')$ for some $\bar{s}'' \in [\![\phi]\!]$, and because of Lemma 6 it must be that $\bar{s}' = \bar{s}''$. Thus $\bar{s}' \in [\![\phi]\!]$, and we can conclude that $\bar{s} \in [\![\uparrow_i \Diamond\phi]\!]$.

For the converse, assume $\omega \in \Downarrow \bar{s}$ for some $\bar{s} \in [\![\uparrow_i \Diamond\phi]\!]$. Then, $\bar{s}'$ exists in $\mathbb{S}$ such that $\bar{s}' \in [\![\phi]\!]$ and $\bar{s}[i] \longrightarrow_i \bar{s}'[i]$. By Definition 8, ω' exists in $\Downarrow(\bar{s}')$, and $\omega \mapsto_i \omega'$ by Definition 4. Finally, by induction hypothesis, $\omega' \in \Downarrow(\bar{s}')$ and $\bar{s}' \in [\![\phi]\!]$ imply that $\omega' \models \phi$.

(case $\uparrow_i \blacklozenge\phi$)

We have that

$$[\![\uparrow_i \blacklozenge\phi]\!] = \{\bar{s} \mid \bar{s}' \in [\![\phi]\!] \text{ exists such that } \bar{s}'[i] \longrightarrow_i \bar{s}[i]\}$$

Assume $\omega \models \uparrow_i \blacklozenge\phi$, and thus $\omega' \mapsto_i \omega$ for some ω' such that $\omega' \models \phi$. By Definition 4, $\omega' \mapsto_i \omega$ implies that $s, s' \in S_i$ exist such that $s' \longrightarrow_i s$, with $\omega \in \downarrow_i(s)$ and $\omega' \in \downarrow_i(s')$. By Lemma 7, $\bar{s}$ and $\bar{s}'$ exist in $\mathbb{S}$ with $\bar{s}'[i] = s' \longrightarrow_i s = \bar{s}[i]$ and such that $\omega \in \Downarrow \bar{s}$ and $\omega' \in \Downarrow \bar{s}'$. Moreover, by induction hypothesis, $\omega' \models \phi$ implies that $\omega' \in \Downarrow(\bar{s}'')$ for some $\bar{s}'' \in [\![\phi]\!]$, and because of Lemma 6 it must be that $\bar{s}' = \bar{s}''$. Thus $\bar{s}' \in [\![\phi]\!]$, and we can conclude that $\bar{s} \in [\![\uparrow_i \blacklozenge\phi]\!]$.

For the converse, assume $\omega \in \Downarrow \bar{s}$ for some $\bar{s} \in [\![\uparrow_i \blacklozenge\phi]\!]$. Then, $\bar{s}'$ exists in $\mathbb{S}$ such that $\bar{s}' \in [\![\phi]\!]$ and $\bar{s}'[i] \longrightarrow_i \bar{s}[i]$. By Definition 8, ω' exists in $\Downarrow(\bar{s}')$, and $\omega' \mapsto_i \omega$ by Definition 4. Finally, by induction hypothesis, $\omega' \in \Downarrow(\bar{s}')$ and $\bar{s}' \in [\![\phi]\!]$ imply that $\omega' \models \phi$.

□

B Experimented Queries for Differential Analysis

Here, we provide more details on the security policy Γ and the queries used in the experiments of Section 4. We created the security policy Γ by considering the three propositions *untrusted*, *secure*, and *critical*, and associating file labels

$$\phi_1 = \uparrow_j \texttt{critical} \Rightarrow \uparrow_i \texttt{critical}$$
$$\phi_2 = \uparrow_j \Diamond \texttt{critical} \Rightarrow \uparrow_i \Diamond \uparrow_j \texttt{critical}$$
$$\phi_3 = \uparrow_j (\texttt{untrusted} \wedge \Diamond \texttt{critical}) \Rightarrow \uparrow_i (\uparrow_j \texttt{untrusted} \wedge \Diamond \uparrow_j \texttt{critical})$$
$$\phi_4 = \uparrow_j (\texttt{untrusted} \wedge \Diamond \texttt{critical}) \Rightarrow \uparrow_i (\texttt{untrusted} \wedge \Diamond \texttt{critical})$$
$$\phi_5 = \uparrow_j (\texttt{untrusted} \wedge \Diamond \texttt{critical}) \wedge \uparrow_i \texttt{untrusted} \Rightarrow \uparrow_i \Diamond \texttt{critical}$$
$$\phi_6 = \uparrow_j (\texttt{critical} \wedge \blacklozenge \texttt{untrusted}) \Rightarrow \uparrow_i (\uparrow_j \texttt{critical} \wedge \blacklozenge \uparrow_j \texttt{untrusted})$$
$$\phi_7 = (\uparrow_j (\Diamond \texttt{critical}) \wedge \uparrow_i \texttt{untrusted}) \Rightarrow \uparrow_j \texttt{secure}$$

Fig. 6: *CML* formulas used for differential analysis of Section 4.

with them according to the following heuristic, which relies on both syntactic and semantic criteria. The syntactic criterion associates a file label with one or more of these propositions if its name contains the name of the proposition as a substring; the semantic criterion associates a label with a proposition if the informal meaning of the label in the Android system corresponds to that of the proposition.

For any analyzed pair of versions i and j of a SEAdroid configuration, we verified the 7 *CML* formulas in Figure 6:

- ϕ_1 says that critical files should not increase, encoding the desired minimality property of the trusted computing base of operating systems;
- ϕ_2 says that files influencing critical resources do not increase, as they can possibly lead to integrity violations;
- ϕ_3 checks that untrusted files influencing critical entities do not increase, thus weakening the previous formula;
- ϕ_4 and ϕ_5 are variations of the previous one discussed in Example 2;
- ϕ_6 checks that critical files influenced by some untrusted entity do not increase, limiting the impact of possibly malicious resources;
- ϕ_7 verifies that files once untrusted, which can now influence critical entities, must be labelled as secure, i.e. it allows declassification only when explicitly documented.