SEApp: Bringing Mandatory Access Control to Android Apps

Matthew Rossi*, Dario Facchinetti*, Enrico Bacis*, Marco Rosa+, Stefano Paraboschi*
*University of Bergamo +SAP Security Research

Objective

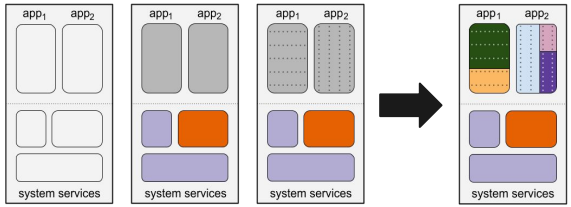
- divide applications in multiple **security contexts**
- **control** the **access** of security contexts to the application internal data
- control the **interactions** among these security contexts

Motivation

Android focuses on isolating applications from each other

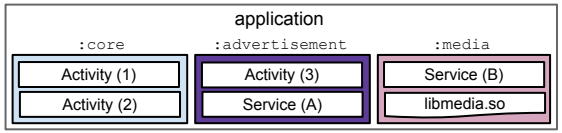
There are no clear means to isolate the internal components of an app:

- every component has **complete access** to the **internal storage**
- 3rd-party libraries may **abuse** app **privileges**
- large and complex **components** prone to bugs are **not easy to isolate**



Idea

- **separate components** into **different** app **processes**
- control with **SELinux** the permissions at process level



Implementation

Apps provide a **fine-grained policy module** to control the permissions granted to processes

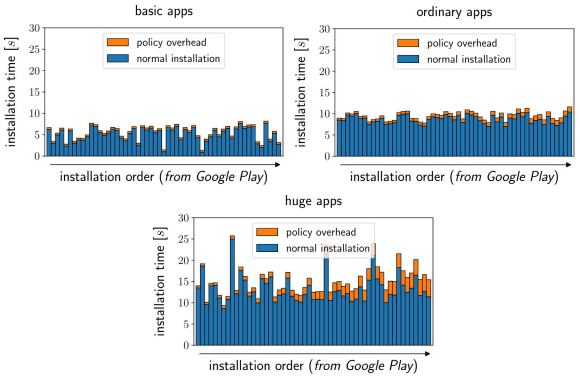
All policy fragments end up in the same **monolithic binary policy**

A **compiler-based** approach **prohibits** the installation of policy modules that may harm the system or other apps

Several changes to:

- **boot** sequence
- app **installation procedure**
- **runtime services** that support the app lifecycle (e.g., Zygote)

Performance evaluation

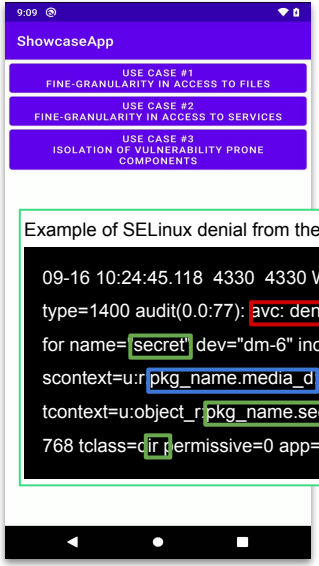


- basic and ordinary policy configurations **exhibit** a **negligible slowdown**, never exceeding 1.22 ± 0.02 s
- **limited overhead** is associated with apps with huge policies, at most 3.59 ± 0.04s

Demonstration

A showcase app affected by common security **vulnerabilities**

- when it is executed by the **Stock OS**, vulnerabilities are **exploitable**
- when it uses the security functions introduced by **SEApp**, the vulnerabilities are **no longer exploitable**



Example of SELinux denial from the log:

```
09-16 10:24:45.118  4330  4330 W pkg.name:media
type=1400 audit(0.0:77): avc: denied { search }
for name="secret" dev="dm-6" ino=5136
scontext=u:r pkg_name.media_d s0:c108,c256,c512,c768
tcontext=u:object_r:pkg_name.secret_t:s0:c108,c256,c512,c
768 tclass=dir permissive=0 app=pkg.nam
```

Availability

ARTIFACT EVALUATED usenix ASSOCIATION PASSED

Open source on GitHub
Tested on physical devices and the Android Emulator