# Improving Android security by widening the role of Mandatory Access Control

Enrico Bacis, Simone Mutti, Marco Rosa, Stefano Paraboschi
{enrico.bacis, simone.mutti, marco.rosa, parabosc} @unibg.it

Università degli Studi di Bergamo

## ABSTRACT

In the evolution of Android, the *Mandatory Access Control* (MAC) at the level of Linux kernel is assuming a central role. In the commonly used *Discretionary Access Control* (DAC), every resource has an owner that defines who can access the resource. In the MAC schema, instead, the access privileges are defined in a global policy, that is enforced by the kernel. Only the system administrator can change the policy, thus preventing many security threats coming from malicious or misbehaving applications.

SELinux is the MAC that has been integrated into Android since version 4.3. Nevertheless it is currently used only to protect system resources from threats originating from applications. Much research studied how to integrate SELinux access control checks into more system components. *AppPolicyModules* [1] allow developers to ship an SELinux module along with the application or to derive an ad-hoc one based on the permissions requested in the application manifest. This improves the protection of the application resources and permits the realization of the classical *least privilege* principle. The project *SeSQLite* [2] integrates SELinux into SQLite databases, both at schema and row level. SQLite is widely used in Android even for system components. *SeSQLite* permits to state that a contact's phone number is more sensitive than the e-mail, even if they are in the same table. Finally, *SEIntentFirewall* [3] leverages SELinux to filter the Intents that an application can send to other applications or to system services.

These improvements tighten the security of Android, providing better protection for the system.

## BODY

*The Android security ecosystem can greatly benefit from a deeper integration of SELinux Mandatory Access Control into system components.*

## REFERENCES

[1] E. Bacis, S. Mutti, and S. Paraboschi. AppPolicyModules: Mandatory Access Control for Third-Party Apps. In *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, pages 309–320. ACM, 2015.

[2] S. Mutti, E. Bacis, and S. Paraboschi. SeSQLite: Security Enhanced SQLite: Mandatory Access Control for Android Databases. In *Proceedings of the 31st Annual Computer Security Applications Conference*, ACSAC 2015, pages 411–420, New York, NY, USA, 2015. ACM.

[3] S. Mutti, E. Bacis, and S. Paraboschi. An SELinux-based Intent manager for Android. In *IEEE Conference On Communications and Network Security*, Florence, Italy, September 2015.

*Volume 4 of Tiny Transactions on Computer Science*