Understanding Android Security
paper summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

To protect applications and data, android uses security enforcement (which is mandetory) at two places, each application executes as its own user identity (system level isolation); and, Android middleware contains a reference monitor that arbitrates the initialization of ICC (inter component communication). This paper focuses on ICC level. The main idea of security enforcement is - assigning permission labels to applications and components. "A reference monitor provides mandatory access control (MAC) enforcement of how applications access components"[1]. It looks at the permission labels assigned to its containing applications, before allowing ICC establishment to be proceed. Paper then provides an exhaustive list of security refinements. Security-aware developers - "should always explicitly define the exported attribute for components intended to be private", "should always assign access permissions to public components", "should specify a permission label to restrict access to the intent object", "should define separate read and write permissions"[1]. Also, Android provides some features such as - protecting sensitive APIs, defining permission protection levels, URI permission and pending intents. Though, the permission label helps in providing security, its assignment to an application provides access to endless resources[1]. Paper concludes with introducing 'Kirin', which checks the permission violations. If application's policy is not complaint, it won't allow the application to get installed[1].

2 Contribution

The paper contributes by introducing a tool (Kirin), "which extracts an application's security policy from its manifest file to determine if the requested permissions and component permission assignments are consistent with the stakeholder's definition of a secure phone"[1].

3 Strengths

The paper is easy to understand. The paper highlights an important issue - A feature of granting permission label, can be act as a security threat, and also gives a remedy.

4 Limitations

Though the title says, 'Understanding Android Security', the paper only concentrates on application level threats, but does not consider the other factors, such as, hardware attacks (eg. Drammer) or man in the middle attacks. Authors have not given any comments on the performance implications of Kirin tool.

5 Future Work

The important challenge is to fix the flaws in 'Kirin' and further investigate android's security. Also, it is important to do a market survey and find similar tools and then integrate them, to make a single standard tool (combining strengths from all of the tools).

References

[1] W. Enck and M. Ongtang and P. McDaniel, *Understanding Android Security*, IEEE Security Privacy, (2009)