

Context-aware Usage Control Mechanism for Securing Android Platform

Guangdong Bai, Liang Gu, Junjun Kong, Yao Guo, Xiangqun Chen
Key Laboratory of High Confidence Software Technologies (Ministry of Education),
Institute of Software, School of EECS, Peking University, Beijing, China.
{baigd08, guliang05, kongjj07, yaoguo, cherry}@sei.pku.edu.cn

Abstract—Existing security mechanism on Android platform is facing great challenges because of the mobility and openness of mobile computing environment. We propose a context-aware usage control model and implement a policy enforcement framework on Android platform. Our model enables smart phone user to express his policy on data protection and resource usage constraint in a fine-grained manner. The implementation of our context-aware usage control mechanism on Android platform leverages the context to enhance its security.

I. INTRODUCTION

Smart phones are serving more and more individuals and enterprises as stretches of desktop computers. Besides security risks and attacks on traditional PCs [1], inherent *personalization, mobility, pay-for-service*, and *limited resource* properties of mobile platform increase the requirement for privacy protection and resource usage constraint in mobile computing environment. It is practical to leverage context information for enhancing security protection and resources usage control. For example, when a user loses his mobile phone, the lost phone detects its unfamiliar context, like a strange location or usage time interval, and then requires an authorization, exposure of the user's privacy will be prevented.

Android holds a coarse-grained and incomplete permission model. It cannot provide data protection and constrain resource usage in a fine-grained manner. What is more, no mechanism for the user to enforce his context-aware constraint on data and resource on Android. To address these two challenges, we propose a context-aware usage control mechanism for Android platform. We extend UCON [2] to a context-aware usage control model. We also implement a policy enforcement framework according to our model on Android platform to enable user to grant permissions in a fine-gained manner. Our mechanism supports revocations and changes on an application's permission at run time. The context-aware usage control mechanism leverages the context information to enhance data protection and resources usage constraint on Android platform.

II. CONTEXT-AWARE USAGE CONTROL MODEL

Our model has three parts: model components, user policy expression and runtime usage decision.

A. Model Components: The model components consist of *subjects* representing applications and components on Android, *objects* representing data, service and resource, *attributes* representing properties of the *subjects* and *objects* related to usage decision, such as UID, right representing access manners for *subjects* to *objects*, like read, write, transmit, *labels* representing permission labels on Android, *state* presenting value set of attributes, *obligation* representing the mandatory action set to perform for *subjects* to access *objects*, *context* representing context value leveraged to enhance security, such as temporal and spatial information.

B. User Policy Expression: User Policy Expression enables the user to express his policy on *objects* taking context and obligation information into account.

C. Runtime Usage Decision: Runtime Usage Decision makes determination based on *state* (i.e. *subject attributes* and *object attributes*), *obligations* and *context* both at the time of usage requests or context switch. It also updates the *state* accordingly.

III. USAGE CONTROL FRAMEWORK

Based on the proposed model, we have implemented a context-aware usage control framework on Android. Figure 1 describes its architecture. When an application sends a request for accessing an object, *Usage Decision* activates *Policy Resolver*, which then resolves corresponding predefined policy according to subject and object. *Usage Decision* also activates *State Evaluation Engine*, *Obligation Evaluation Engine*, and *Context Evaluation Engine* at the same time. *Policy Resolver* then sends its resolving result to these three *Evaluation Engines*. They check fulfillment of *state*, *obligation* and *context* and send result back to *Usage Decision*, which then authorizes the access or not.

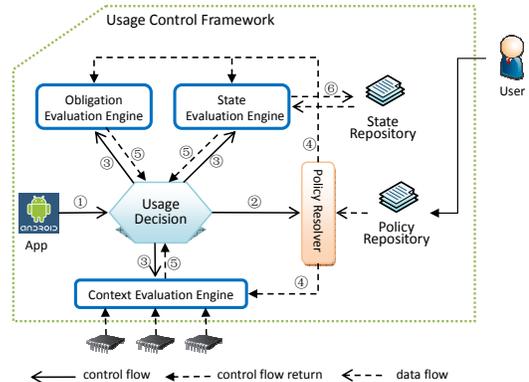


Figure 1. Context-aware Usage Control Framework on Android

IV. CONCLUSION AND FUTURE WORK

Our context-aware usage control framework enhances the security and resource usage on Android platform. We will further study its application for more real usages. Meanwhile, our mechanism also holds for other types of mobile computing platform. We will apply it for other mobile computing systems.

REFERENCES

- [1] Mikko Hypponen. Mobile Malware. USENIX Security Symposium, August 2007. Invited Talk.
- [2] Jaehong Park and Ravi Sandhu. The UCON_{ABC} usage control model. *ACM Transactions on Information and System Security*, 7(1):128–174, February 2004.