Privacy-Preserving Mobile Access to Personal Health Records through Google's Android

Vassiliki Koufi[1], Flora Malamateniou[1], George Vassilacopoulos[1,2]

[1]Department of Digital Systems
University of Piraeus
Piraeus, Greece
{vassok, flora, gvass}@unipi.gr

[2]New York University
New York, NY

***Abstract*—Nowadays, physicians are increasingly utilizing mobile health (mHealth) applications in clinical care. Despite their attractive features, mHealth applications may pose substantial risks to the privacy and security of personal health information. This paper presents an access control framework which is incorporated in PHRManager, an Android-enabled application providing ubiquitous access to patient Personal Health Records (PHRs) by authorized users (i.e. patients themselves and attending healthcare professionals).**

Keywords- mobile device, Android, Personal Health Record, attribute-based access control, privacy

I. INTRODUCTION

PHRManager is an application that meets information and knowledge needs of both healthcare professionals and patients by rendering patients' PHRs ubiquitously accessible in a timely and, where possible, transparent manner via any Android-enabled device[1]. This paper presents the access control framework incorporated in PHRManager. The proposed framework mediates communication between users and application components as well as between application components in order to achieve privacy-preserving information flow during transactions. Moreover, it adheres to the attribute-based access control paradigm, which, as opposed to other approaches, does not incur any significant administrative overhead and is self-administering to a great extent.

II. SYSTEM ARCHITECTURE

Figure 1 illustrates a high-level view of the system architecture in terms of a three-tier model which comprises PHRManager native Android applications, the access control mediator and Linux kernel. In particular, the first layer contains the Android application packages (apk) and attribute-based access control (ABAC) policies relevant to each individual application. The mediator residing at the middle layer enforces access control over the Android applications. Essentially, it comprises three components, namely AttributeCollector, PolicyAuthority and PolicyEnabler, and complements the native component which enforces access control in Android Systems. Upon request for data access by an Android application, an Inter-Component Communication (ICC) event is initiated through the middleware framework. The ICC is intercepted by the PolicyEnabler before it reaches the Android standard access control mechanism. PolicyEnabler queries the PolicyAuthority for policies that match the entities involved in the ICC (i.e. Requestor, Resource). The PolicyAuthority identifies all the relevant policies, evaluates them against the entity attribute values obtained by the AttributeCollector, and returns the decision to PolicyEnabler. If the policy conditions are satisfied, the ICC is directed by the PolicyEnabler to the native Android access control module and the requested information is retrieved by the requesting party. Otherwise the ICC is blocked.

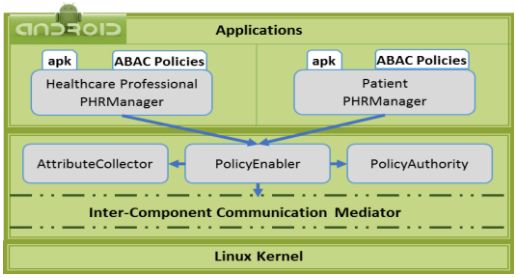

Figure 1. System architecture

III. IMPLEMENTATION

The components comprising the PHRManager access control mechanism have been implemented in a prototype native Android application using Android SDK 4.0.3r2 API15, while the ABAC policies have been defined using eXtensible Access Control Markup Language (XACML) [2][3].

IV. CONCLUSIONS

PHRManager is a high-performance Android-enabled mobile framework which enables healthcare professionals to cope more efficiently with their day-to-day activities and patients to manage their health with the least possible intervention. Through the framework presented in this paper, this can be achieved without breaching patient privacy.

REFERENCES

[1] V. Koufi, F. Malamateniou, A. Tsohou, and G. Vassilacopoulos, "An Android-Enabled Mobile Framework for Ensuring Quality of Life through Patient-Centric Care," in Proceedings of MIE 2012. Pizza, Italy.

[2] "Android," [Online]. Available: http://www.android.com/

[3] OASIS, "eXtensible Access Control Markup Language (XACML)." [Online] Available: https://www.oasis-open.org/

MOBIHEALTH 2014, November 03-05, Athens, Greece

DOI 10.4108/icst.mobihealth.2014.257532