Chapter 20
Preserving User Privacy and Security in Context-Aware Mobile Platforms

Prajit Kumar Das
University of Maryland – Baltimore County, USA

Dibyajyoti Ghosh
University of Maryland – Baltimore County, USA

Pramod Jagtap
University of Maryland – Baltimore County, USA

Anupam Joshi
University of Maryland – Baltimore County, USA

Tim Finin
University of Maryland – Baltimore County, USA

ABSTRACT

Contemporary smartphones are capable of generating and transmitting large amounts of data about their users. Recent advances in collaborative context modeling combined with a lack of adequate permission model for handling dynamic context sharing on mobile platforms have led to the emergence of a new class of mobile applications that can access and share embedded sensor and context data. Most of the time such data is used for providing tailored services to the user but it can lead to serious breaches of privacy. We use Semantic Web technologies to create a rich notion of context. We also discuss challenges for context aware mobile platforms and present approaches to manage data flow on these devices using semantically rich fine-grained context-based policies that allow users to define their privacy and security need using tools we provide.

DOI: 10.4018/978-1-5225-8897-9.ch020

INTRODUCTION

Smartphones or mobile devices that run advanced mobile operating systems are transforming how we communicate with people and connect with the world. Modern mobile operating system platforms like Android and iOS provide applications or "apps" through their "marketplaces". Combining computing ability with apps allows a "smart" phone to accomplish tasks that would either require a personal computer or special hardware components. For example a user can take pictures, record a video, connect to the Internet, navigate using GPS, prepare a presentation and accomplish many other day-to-day tasks, on smartphones.

However, with great power that comes with substantial computing and special hardware based sensing ability of smartphones, comes with added risks to user data. Advanced sensing abilities on smartphones have given rise to a new generation of intelligent applications. Smart assistants like Siri, Google Now and Microsoft Cortana are just a few examples of intelligent applications that are context-aware. All such apps exploit a user's location context to deliver personalized services. They do this by leveraging the user's location at the level of position, i.e., geospatial (latitude-longitude) coordinates. Integrating this with readily available background knowledge allows such systems to identify the location with a known place (e.g., Baltimore), facility (e.g., the BWI airport) or an organization (e.g., UMBC). As a result, location becomes an important aspect of a user's context but there are additional contextual information that includes a user's activity, identity and temporal information (Dey & Abowd, 1999). Naturally, protecting the security and privacy of user data now includes the critical task of protecting contextual data. In this chapter, we will discuss access control issues that need to be focused on and discuss solutions that have been proposed by researchers in the domain.

BACKGROUND

Access control generally refers to the process of determining what actions are allowed by a given subject upon objects and resources (Sandhu & Samarati, 1996). The security domain has seen the emergence of various access control models over the years. The most popular models include Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role Based Access Control (RBAC) and Attribute Based Access Control (ABAC). DAC refers to access control mechanisms where it is at the "discretion" of the owner of an object. On the other hand, MAC "mandates" control based on security labels assigned to an object. RBAC is a model that uses "roles" to determine access control and in this model permissions are associated with roles, and users are made members of appropriate roles. RBAC suffers from issues of setting up initial role structure and inflexibility in dynamic domains (Kuhn, D. R., Coyne, E. J., & Weil, T. R., 2010). A pure RBAC solution will not consider dynamic attributes like time of day, which could be critical for determining user permissions. Essentially, it does not take into consideration the context aspect that we so often see, especially in the mobile domain. ABAC models are better equipped in handling access control for such dynamic systems. When it comes to using ABAC models one of the standard system implementations created by (Godik, S., Anderson, A., Parducci, B., Humenn, P., & Vajjhala, S., 2002) is XACML. The XACML standard defines a declarative access control policy language implemented in XML and provides a processing model on how to evaluate access requests. The access control mechanisms that we will discuss are modeled on ABAC.

Related Content