Context-Based Access Control Systems for Mobile Devices

Bilal Shebaro, Oyindamola Oluwatimi, and Elisa Bertino, Fellow, IEEE

* Research problem

Mobile Android applications often have access to sensitive data and resources on the user device. Misuse of this data by malicious applications may result in privacy breaches and sensitive data leakage.

* Research objective(s)

As smartphones are becoming more powerful in terms of computational and communication capabilities, application developers are taking advantage of these capabilities in order to provide new or enhanced services to their applications.

Study Context & Methodology/Experimental Design

Propose a context-based access control (CBAC) mechanism for Android systems that allows smart- phone users to set configuration policies over their applications’ usage of device resources and services at different contexts. Through the CBAC mechanism, users can, for example, set restricted privileges for device applications when using the device at work, and device applications may re-gain their original privileges when the device is used at home. This change in device privileges is automatically applied as soon as the user device matches a pre- defined context of a user-defined policy. The user can also specify a default set of policies to be applied when the user is located in a non-previously defined location.

* Results

Users to configure their own set of policies; the difficulty of setting up these configurations require the same expertise needed to inspect application permissions listed at installation time. However we plan to extend our approach to give network administrators of organizations the same capabilities once a mobile device connects to their network. In this way, network administrators are able to block malicious application accesses to resources and services that may affect the security of their network. We believe that such an approach is critical for assuring security of corporate networks when organizations allow users to “bring their own devices”.

* Main points/arguments
* 1)  Applications should not be able to fake the location or time of the device, as they should not be able to bypass the policy restrictions applied on the device in a specific context.
* 2)  As users are assumed to be mobile, the policy restrictions should be applied automatically on the device as the device’s location changes.
* 3)  The accuracy of location needs to be higher than the location accuracy by GPS, as we need to apply different policies in different spots or nearby sub-areas located within the same GPS location.
* 4)  The enforcement of context-based policies should not require the application developers to modify source code, or impose any additional requirement on their applications.
* 5)  The applied policy should not cause significant delays in the device functionality that could negatively impact the system performance.
* Quality of related work

Several approaches have been proposed for context- based access control. Generalized Role Based Access Control (GRBAC) is an approach that incorporates the concept of environment information (such as time) into access control. GRBAC is very expressive and thus suitable for context aware authorization.

* Strengths/ Weaknesses

Relates to techniques for providing reliable location information that can provide adequate security guarantees once merged with security policies. GPS is the most commonly used technology for location purposes. However it is not very reliable when used indoor due to its low signal power. Related to techniques implemented for the Android OS to restrict device applications for protecting the user privacy and device security.

* Significance & Contributions

Proposed a modified version of the Android OS supporting context-based access control poli- cies. These policies restrict applications from accessing spe- cific data and/or resources based on the user context. The restrictions specified in a policy are automatically applied as soon as the user device matches the pre-defined context associated with the policy. Our experimental results show the effectiveness of these policies on the Android system and applications, and the accuracy in locating the device within a user-defined context.