**CONTEXT-BASED ACCESS CONTROL SYSTEMS FOR MOBILE DEVICES**

**ABSTRACT:**

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. An example would be a malicious application surreptitiously recording a confidential business conversation. The problem arises from the fact that Android users do not have control over the application capabilities once the applications have been granted the requested privileges upon installation. In many cases, however, whether an application may get a privilege depends on the specific user context and thus we need a context-based access control mechanism by which privileges can be dynamically granted or revoked to applications based on the specific context of the user. In this paper we propose such an access control mechanism. Our implementation of context differentiates between closely located sub-areas within the same location. We have modified the Android operating system so that context-based access control restrictions can be specified and enforced. We have performed several experiments to assess the efficiency of our access control mechanism and the accuracy of context detection.

**EXISTING SYSTEM:**

Security for mobile operating systems focuses on restricting applications from accessing sensitive data and resources, but mostly lacks efficient techniques for enforcing those restrictions according to fine-grained contexts that differentiate between closely located subareas. Moreover, most of this work has focused on developing policy systems that do not restrict privileges per application and are only effective system-wide. So User disable all applications from using the camera and any device resources and privileges that employers restrict while at work, while the user device can retain all its original privileges outside the work area.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Do not cover all the possible ways in which applications can access user data and device resources.
* The User leakage of Their privacy.
* Existing location-based policy systems are not accurate enough to differentiate between nearby locations without extra hardware or location devices.

**PROPOSED SYSTEM:**

In this paper, we propose a context-based access control (CBAC) mechanism for Android systems that allows smartphone 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. Configured policy restrictions are defined according to the accessible device resources, services, and permissions that are granted to applications at installation time. Such policies define which services are offered by the device and

limit the device and user information accessibility. Policy restrictions are linked to context and are configured by the device user. We define context according to location and time.

**ADVANTAGES OF PROPOSED SYSTEM:**

* Applications should not be able to fake the location or time of the device.
* Can develop securer and more acceptable applications for end users.

**SYSTEM ARCHITECTURE:**

****

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.
* MOBILE : ANDROID

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/7.
* Coding Language : Java 1.7
* Tool Kit : Android 2.3 ABOVE
* IDE : Eclipse

**REFERENCE:**

Bilal Shebaro, Oyindamola Oluwatimi, Elisa Bertino, “Context-based Access Control Systems for Mobile Devices”, IEEE Transactions on Dependable and Secure Computing, 2014.