Access Control Models on Mobile Devices

This abstract contains introduction to the Privacy Protection on Mobile Devices which includes security access. There is a wide range of approaches to do a research in this area. In this talk I would like to present a problem of security access to the sensitive information on a file systems. Consider a security compromise to be unauthorized access to the information, where *unauthorize* means that an inappropriate clearance of a lack of need-to-know is involved in the access to information. Then a main problem to be solved within the computing system is how to guarantee that unauthorized access (by a process) to the information (file, program, data) does not occur.

Primarily this approach is commonly designed by Access Control Models. These models are sometimes categorized as either discretionary or non-discretionary. Three most widely recognized models are Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC). MAC is non-discretionary and rest of these models is discretionary. There are many different mobile operating systems but they use similar methods to secure a privacy user data called MAC. It refers to allowing access to a resource if and only if rules exist that allow a given user to access the resource. It is difficult to manage, but it is usually used to protect the highly sensitive information. Examples include certain government and military information. This manner is used on mobile devices which only owner is the unique user of device.

The aim of the presentation is to show the differences between these models and to present the most widely used model on mobile devices. Discussion will also contain formal description of well-known Bell and LaPadula Model which is a basic model of Access Control Models. This model of protection systems deals with the control of information flow. It is a linear non-discretionary model. This model of protection consists of the following components: set of *subjects*, set of *objects* and an access control matrix.

Lukáš Aron
iaron@fit.vutbr.cz

Department of Intelligent Systems
Faculty of Information Technology
Brno University of Technology
Brno, Czech republic