The PEI + UCON Framework for Application Security

Ravi Sandhu
Executive Director and Endowed Professor of Cyber Security
Institute for Cyber Security, University of Texas at San Antonio
ravi.sandhu@utsa.edu, www.profsandhu.com

There is no security without application context. Only application context can make clear the tradeoffs between security, performance, usability and cost, and further the tradeoffs between conflicting security objectives such as confidentiality, integrity and availability. To capture application security policy we need a more sophisticated model than traditional access control provides. To this end we developed a model called UCON [2] depicted in figures 1 and 2. UCON is attribute-based but goes beyond traditional attribute-based models in that attributes are mutable and can change automatically as a side-effect of access (or usage). Moreover, UCON accommodates the notions of obligations and conditions which capture additional requirements beyond authorization. Obligations require some action such as clicking on an Agree button before access is granted. Conditions capture system and environmental attributes not directly tied to the subject or object in question. The three cornerstones of UCON, authorizations, obligations and conditions can be applied before, during and after access. The goal of UCON was to unify several different access control extensions that had been published or implemented. Thus far the applications of UCON have not required us to extend it in any fundamental way, although we continue to look for applications that stress UCON so we may discover important extensions.

Having a rich and expressive model is not sufficient to design and implement secure applications. We also need a methodology. We have developed the PEI methodology illustrated in figure 3. This methodology clearly separates three layers in the design process [1, 4]. These are the Policy layer, Enforcement layer and Implementation layer. At each layer we need a formal model to express the application policy. At the P layer this policy is developed in an idealized context where it is assumed all attributes required to make access decisions are available and up to date. This corresponds to an idealized centralized system where everything is together in one computer. The E layer deals with the approximations and additional servers introduced by the distributed nature of real-world systems. The goal is to make the approximations explicit and controllable since perfect correspondence to the idealized P layer is impossible. Finally the I layer spells out detailed implementation protocols and mechanisms. In particular UCON is well suited to the P and E layers, whereas the I layer requires different scope of models. It should be mentioned that PEI is an evolution of the earlier OM-AM framework [3].

We have applied UCON and PEI to numerous application problems. Most recently our focus has been on group-centric information sharing. We are looking for collaborators to develop UCON-based models in different application and technology contexts.

References


Figure 2. Continuity & Mutability Properties of UCON.

Figure 3. The PEI Models Framework.