Panel

Future Direction of Access Control Models, Architectures, and Technologies

Moderator:
Konstantin Beznosov
University of British Columbia

Description

Are we witnessing the beginning of the end for Access Control, as the research community knew it twenty and maybe even ten years ago? We find ourselves dealing with drastically new trust and threat models, very different target applications, and requirements for supported policies.

Trusted Computing Base (TCB) is disappearing in the Untrusted Computing Base (UCB), Reference Monitor becomes more and more application specific and gets distributed and inter-wined with the business logic. Content has to be protected in the hostile environment of the consumer's laptop, (i)Pod, PDA, cell phone, or DVD player. Clear and rigid models of MAC with nice properties are being traded for expressible and extensible languages that can code almost any Turing Machine. Simple homogeneous course-grain file-oriented resources are being replaced with complex heterogeneous and fine-grained objects and XML-documents.

Instead of making things simpler, the community seems to ignore the Einstein's wisdom and keeps looking for the ways to make them more complex. The security community in general and the access control one in particular find themselves looking for the ways to support:

- Decentralized P2P applications where everybody is their own policy authority and yet need to have their policies to scale to millions of peers,
- DRM applications with continuing enforcement of owners' policies on the consumer devices with no guarantee, whatsoever, of any TCB presence,
- Privacy policies with unverifiable purposes determined by end users,
- Authorization of strangers and other trust (or lack of it) management scenarios.

The goal of this panel is to explore future directions in the research and practice of Access Control Models, Architectures, and Technologies (ACMAT). The panelists will offer their (speculative) opinions on what direction the field of Access Control is evolving to. Specific topics addressed by the panel are as the follows:

- Target environments: How are the environments, in which access control technologies are deployed, going to change in the future? Will Palladium and alike give us more hope for the return of TCB, or should we accept the dominance of DRM-like environments? To this end, would the lack or presence of TCB make any difference for ACMAT?
- Target applications: What should we expect next after Grids, P2P, DRM, Web services, as target applications for access control?
- Simple or complex: Is the ever-increasing complexity of ACMAT solutions the sign of our ineptness, and the community should strive to simplify things? Or, the complexity is the only way forward given the intricacy of the target applications?
- Paradigm shift: Will the future developments bring us new fundamental results (similar to access matrix, capabilities, and ACLs, BLP, RBAC, etc.) or more new applications of the existing models and architectures? Should we expect (or hope for) paradigm changes in ACMAT?
- Should the access control community keep searching for technological solutions to their (likely unsolvable) problems, or it should turn to regulatory and other social mechanisms? At the end of the day, the locks on our house/apartment doors are quite simple, thanks to the laws, regulations, and police. What will be "good enough" ACMAT in the future?

SACMAT'05, June 1–3, 2005, Stockholm, Sweden.
ACM 1-59593-045-0/05/0006.