DEPARTMENT OF COMPUTER SCIENCE
THE UNIVERSITY OF WESTERN ONTARIO

Public Lecture for the Degree of Ph.D.

Daniel Servos

Hierarchical Group and Attribute-Based Access Control: Incorporating Hierarchical Groups and Delegation into Attribute-Based Access Control

---

DATE:	Thursday, March 12, 2020
TIME:	10:00 am
PLACE:	MC 320
THESIS SUPERVISOR:	Dr. Mike Bauer
EXTRA-DEPARTMENTAL	
EXAMINER:	Dr. Abdelkader Ouda, ECE
EXTERNAL EXAMINER:	Dr. Ravi Sandhu, Univ of Texas at S.A.
THESIS EXAMINERS:	Dr. Hanan Lutfiyya
	Dr. Kostas Kontogiannis

ABSTRACT

Attribute-Based Access Control (ABAC) is a promising alternative to traditional models of access control (i.e. Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role-Based Access control (RBAC)) that has drawn attention in both recent academic literature and industry application. However, formalization of a foundational model of ABAC and large-scale adoption is still in its infancy. The relatively recent popularity of ABAC still leaves a number of problems unexplored. Issues like delegation, administration, auditability, scalability, hierarchical representations, etc. have been largely ignored or left to future work. This thesis seeks to aid in the adoption of ABAC by filling in several of these gaps.

The core contribution of this work is the Hierarchical Group and Attribute-Based Access Control (HGABAC) model, a novel formal model of ABAC which introduces the concept of hierarchical user and object attribute groups to ABAC. It is shown that HGABAC is capable of representing the traditional models of access control (MAC, DAC and RBAC) using this group hierarchy and that in many cases it's use simplifies both attribute and policy administration. HGABAC serves as the basis upon which extensions are built to incorporate delegation into ABAC.

Several potential strategies for introducing delegation into ABAC are proposed, categorized into families and the trade-offs of each are examined. One such strategy is formalized into a new User-to-User Attribute Delegation model, built as an extension to the HGABAC model. Attribute Delegation enables users to delegate a subset of their attributes to other users in an "off-line" manner (not requiring connecting to a third party).

Finally, a supporting architecture for HGABAC is detailed including descriptions of services, high-level communication protocols and a new low-level attribute certificate format for exchanging user and connection attributes between independent services. Particular emphasis is placed on ensuring support for federated and distributed systems. Critical components of the architecture are implemented and evaluated with promising preliminary results.

It is hoped that the contributions in this research will further the acceptance of ABAC in both academia and industry by solving the problem of delegation as well as simplifying administration and policy authoring through the introduction of hierarchical user groups.