Procceedings IFIP/IEEE International Workshop on Distributed Systems: Operations and Management, October 15-16 1991, Santa Barbara, CA

Decentralized Management of Security in Distributed Systems

Ravi S. Sandhu

Center for Secure Information Systems
and
Department of Information and Software Systems Engineering
George Mason University, Fairfax, VA 22030-4444
sandhu@sitevax.gmu.edu

[Extended Abstract]

1 INTRODUCTION

Security and trust are fundamental issues which must be considered in the management and operation of distributed systems. Controlled autonomy of component systems is an intrinsic aspect of large-scale distributed systems. The alternatives to controlled autonomy are total anarchy or rigid centralized control.

Autonomy implies that each component system should have the ability to specify the security policy with respect to resources that it controls. The composition of these multiple security policies into a coherent system-wide policy is a major challenge in the management of distributed systems. Autonomy also implies that the security officer of each component system has discretion regarding the trust invested in other component systems. The individual security officers of component systems should be free within specified parameters to configure the security policy of their system and its interactions with other components. At the same time it should be possible to analyze the net global result of these individual decisions. Analyzing the composition and interaction of security policies is therefore extremely important in a distributed environment with multiple autonomous points of security control.

Much of the classical research and development in computer security has occurred in context of centralized systems. These systems postulate a security officer who is in effect a "security czar" having complete control over the security aspects of the system. In distributed systems we must go beyond this traditional view to consider systems which have multiple autonomous points of security control.

2 THE SCHEMATIC PROTECTION MODEL

GMU researchers have been active for several years in the study of decentralized security controls and their composition into a coherent system-wide policy. Sandhu's Schematic Protection Model (SPM) [8] is a formal access control model developed for this purpose. The initial focus of this research was on the "safety analysis" of SPM. Safety analysis is the key to understanding whether the composition of multiple autonomous security policies gives us an acceptable global system-wide policy. A notable property of SPM is that it has efficient safety analysis under very general assumptions (specifically the can-create relation on subject types has to be acyclic [8]). The expressive of this model has been amply demonstrated [9]. Ammann and Sandhu [1, 2] have also recently shown that SPM extended with multi-parent creation (ESPM) has the complete expressive power of the monotonic access-matrix model, while retaining the efficient safety analysis of SPM.

Recently we have been looking at distributed implementations of SPM. We first considered a special case of SPM called the Transform Model [10] and developed a distributed capability based architecture for it [11]. We then proposed a distributed capability-based architecture for the full-fledged ESPM model [3].

3 SUMMARY

At the workshop we will present the Schematic Protection Model, and its variations, and discuss their application for security management in distributed systems. We will also present the implementation architectures we have developed and compare these with other work on secure distributed system architectures (e.g., [4, 5, 6, 7]).

References

[1] Ammann, P. and Sandhu, R.S. "Extending the Creation Operation in the Schematic Protection Model." *Proc. Sixth Annual Computer Security Applications Conference*, Tucson, Arizona, December 1990, pages 340-348.

[2] Ammann, P. and Sandhu, R.S. "Safety Analysis for the Extended Schematic Protection Model." *Proc. IEEE Symposium on Research in Security and Privacy*, Oakland, California, May 1991, to appear.

[3] Ammann, P.E., Sandhu, R.S. and Suri, G.S. "A Distributed Implementation of the Extended Schematic Protection Model." *Seventh Annual Computer Security Applications Conference*, San Antonio, Texas, December 1991, to appear.

[4] Gasser, M., Goldstein, A., Kaufman, C., Lampson, B. "The Digital Distributed System Security Architecture." *IEEE Symposium on Security and Privacy*, 305-319 (1989)

[5] Gong, L. "A Secure Identity-Based Capability System." *IEEE Symposium on Security and Privacy*, 56-63 (1989).

[6] Mullender, S.J., Tanenbaum, A.S. and van Renesse, R "Using Sparse Capabilities in Distributed Operating Systems." *6th International Conference on Distributed Computing Systems*, (1986).

[7] Mullender, S.J., van Rossum, G., Tanenbaum, A.S., van Renesse, R. and van Staveren, H. "Amoeba: A Distributed Operating System for the 1990s." *IEEE Computer*, 23(5):44-53 (1990).

[8] Sandhu, R.S. "The Schematic Protection Model: Its Definition and Analysis for Acyclic Attenuating Schemes." *Journal of the ACM*, Volume 35, Number 2, April 1988, pages 404-432.

[9] Sandhu, R.S. "Expressive Power of the Schematic Protection Model." *Proc. IEEE Computer Security Foundations Workshop I*, Franconia, New Hampshire, June 1988, pages 188-193.

[10] Sandhu, R.S "Transformation of Access Rights" *IEEE Symposium on Security and Privacy*, 259-268 (1989).

[11] Sandhu, R.S. and Suri, G.S. "A Distributed Implementation of the Transform Model." *14th NIST-NCSC National Computer Security Conference*, Washington, D.C., October 1991, to appear.