Role-Based Access Controls

Reprinted from
15th National Computer Security Conference (1992)
Baltimore, Oct 13-16, 1992. pp. 554 - 563

David F. Ferraiolo and D. Richard Kuhn
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce
Gaithersburg, Md. 20899 USA

ABSTRACT

While Mandatory Access Controls (MAC) are appropriate for multilevel secure military applications, Discretionary Access Controls (DAC) are often perceived as meeting the security processing needs of industry and civilian government. This paper argues that reliance on DAC as the principal method of access control is unfounded and inappropriate for many commercial and civilian government organizations. The paper describes a type of non-discretionary access control - role-based access control (RBAC) - that is more central to the secure processing needs of non-military systems than DAC.

Keywords: access control, computer security, discretionary access control, integrity, mandatory access control, role, TCSEC

1 Introduction

The U.S. government has been involved in developing security technology for computer and communications systems for some time. Although advances have been great, it is generally perceived that the current state of security technology has, to some extent failed to address the needs of all. [1], [2] This is especially true of organizations outside the Department of Defense (DoD). [3]

The current set of security criteria, criteria interpretations, and guidelines has grown out of research and development efforts on the part of the DoD over a period of twenty plus years. Today the best known U.S. computer security standard is the Trusted Computer System Evaluation Criteria (TCSEC [4]). It contains security features and assurances, exclusively derived, engineered and rationalized based on DoD security policy, created to meet one major security objective - preventing the unauthorized observation of classified information. The result is a collection of security products that do not fully address security issues as they pertain to unclassified sensitive processing environments. Although existing security mechanisms have been partially successful in promoting security solutions outside of the DoD [2] , in many instances these controls are less then perfect, and are used in lieu of a more appropriate set of controls.