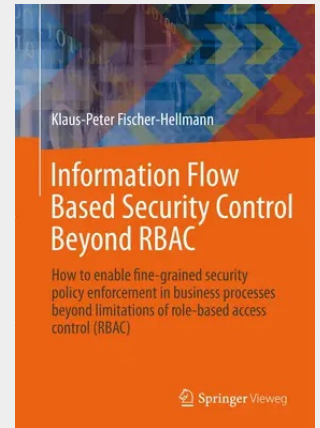


Information Flow Based Security Control Beyond RBAC

How to enable fine-grained security policy enforcement in business processes beyond limitations of role-based access control (RBAC)

Role-based access control (RBAC) is a widely used technology to control information flows as well as control flows within and between applications in compliance with restrictions implied by security policies, in particular, to prevent disclosure of information or access to resources beyond restrictions defined by those security policies. Since RBAC only provides the alternatives of either granting or denying access, more fine-grained control of information flows such as "granting access to information provided that it will not be disclosed to targets outside our organisation during further processing" is not possible. In business processes, in particular those spanning several organisations, which are commonly defined using business process execution language (BPEL), useful information flows not violating security policy-implied limitations would be prevented if only the access control capabilities offered by RBAC are in use. The book shows a way of providing more refined methods of information flow control that allow for granting access to information or resources by taking in consideration the former or further information flow in a business process requesting this access. The methods proposed are comparatively easy to apply and have been proven to be largely machine-executable by a prototypical realisation. As an addition, the methods are extended to be also applicable to BPEL-defined workflows that make use of Grid services or Cloud services. IT Security Specialists Chief Information Officers (CIOs) Chief Security Officers (CSOs) Security Policy and Quality Assurance Officers and Managers Business Process and Web/Grid/Cloud Service Designers, Developers, Operational Managers Interested Learners / Students in the Field of Security Management.

Role-based access control (RBAC) is a widely used technology to control information flows as well as control flows within and between applications in compliance with restrictions implied by security policies, in particular, to prevent disclosure of information or access to resources beyond restrictions defined by those security policies. Since RBAC only provides the alternatives of either granting or denying access, more fine-grained control of information flows such as "granting access to information provided that it will not be disclosed to targets outside our organisation during further processing" is not possible. In business processes, in particular those spanning several organisations, which are commonly defined using business process execution language (BPEL), useful information flows not violating security policy-implied limitations would be prevented if only the access control capabilities offered by RBAC are in use. The book shows a way of providing more refined methods of information flow control that allow for granting access to information or resources by taking in consideration the former or further information flow in a business process requesting this access. The methods proposed are comparatively easy to apply and have been proven to be largely machine-executable by a prototypical realisation. As an addition, the methods are extended to be also applicable to BPEL-defined workflows that make use of Grid services or Cloud services. IT Security Specialists Chief Information Officers (CIOs) Chief Security Officers (CSOs) Security Policy and Quality Assurance Officers and Managers Business Process and Web/Grid/Cloud Service Designers, Developers, Operational Managers Interested Learners / Students in the Field of Security Management.



53,49 €

49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783834826176

Medium: Buch

ISBN: 978-3-8348-2617-6

Verlag: Springer

Erscheinungstermin: 02.11.2012

Sprache(n): Englisch

Auflage: 1. Auflage 2012

Serie: IT im Unternehmen

Produktform: Kartoniert

Gewicht: 321 g

Seiten: 161

Format (B x H): 168 x 240 mm

