سومین کنفرانس فناوری اطلاعات و دانش
۶ تا ۸ آذرماه ۱۳۸۶
IKT 2007 کنفرانس بین المللی فناوری اطلاعات و دانش
دانشگاه فردوسی مشهد

ارائه مدلی برای تفکیک وظایف در سیستم‌های کنترل دسترسی بر مبنای نقش

محمد داورپناه جزی، محمد حسین سرایی و مجید سعیدی مبارکه

دانشکده برق و کامپیوتر دانشگاه صنعتی اصفهان، دانشگاه آزاد اسلامی واحد نجف آباد

E-mail: msaidim@yahoo.com, saraee@cc.iut.ac.ir, mdjazi@cc.iut.ac.ir

چکیده - این مقاله پس از شرح مختصر مدل‌های موجود تفکیک وظایف در سیستم‌های کنترل دسترسی بر مبنای نقش از جمله استاندارد *ANSI INCITS 359-2004* و بیان کمبودهای آنها به ارائه مدلی به نام *CBSD (Cardinality-Based Separation of Duties)* می‌پردازد. پس از توصیف رسمی مدل و بیان برخی مزایای آن، با مثالی چگونگی به کارگیری مدل پیشنهادی در سازمان‌ها تشریح می‌شود. در کنار مدل، الگوریتم‌هایی جهت تشخیص تضاد بین قیود تفکیک وظایف، استنتاج نقش‌های قابل انتساب یا باز پس‌گیری هر کاربر و ساده‌سازی قیود تعریف شده معرفی می‌شود. برای نمایش کاربردی بودن مدل و الگوریتم‌های ارائه شده نرم‌افزاری به نام *CBSDT (Cardinality-Based Separation of Duties Tool)* تولید شده که مختصراً شرح داده می‌شود. نهایتاً پیشنهاداتی به منظور توسعه مدل ارائه می‌شود.

کلید واژه - تفکیک وظایف، کنترل دسترسی، کنترل دسترسی بر مبنای نقش.

1- مقدمه

در مبحث کنترل دسترسی بر مبنای نقش، تفکیک وظایف از اهمیت ویژه‌ای برخوردار بوده و یک مکانیزم قوی برای طراحی سیاست‌های سازمانی در حوزه انتساب نقش‌ها به کاربران در جهت کاهش احتمال سوء استفاده از منسب‌ها می‌باشد [1]. طبق تعریف، تفکیک وظایف ابزاری است برای اطمینان از این که سوء استفاده و کلاه برداری در سیستم تنها با تبانی اشخاص قابل حصول بوده و انتساب نقش‌ها به گونه‌ای است که امکان هیچ کلاه برداری در سیستم به صورت شخصی وجود ندارد [1]. در تفکیک وظایف سعی بر این است نقش‌هایی که به گونه‌ای مستعد سوء استفاده هستند را به افراد مختلف اعطا کنیم تا یک فرد نتواند از ترکیب نقش‌های خود سوء استفاده کند. قیود تعریف شده برای تفکیک وظایف، عبارت‌هایی هستند که در موقع انتساب یک نقش به کاربر (تفکیک ایستای وظایف) یا در موقع فعال سازی نقش‌های متعلق به کاربر (تفکیک پویای وظایف) وارد عمل شده و صحت انتساب یا فعال سازی را بررسی می‌کنند. در صورتی که عملیات مورد نظر با قیود تعریف شده سازگار باشد می‌تواند انجام شود. در غیر این صورت از اجرای آن جلوگیری می‌شود. به این صورت اطمینان خواهیم داشت که کاربران سیستم در هر لحظه نقش‌هایی سازگار با سیاست‌های سازمان خواهند داشت.

2- نیازهای تفکیک وظایف

با توجه به مدل‌های موجود در مراجع [2] الی [11] نیازهای تفکیک وظایف در سیستم‌های کنترل دسترسی بر مبنای نقش را می‌توان حمایت از پیشنیازی انتساب یک نقش به کاربر برای انتساب نقش دیگری به او، حمایت از ممنوعیت انتساب یک نقش به کاربر برای انتساب نقش دیگری به او، حمایت از عملگرهای منطق بولی (and, or, not) در بیان سیاست‌های سازمانی انتساب نقش‌ها به کاربران، حمایت از کاردینالیتی انتساب نقش‌ها به کاربران، حمایت از کاردینالیتی انتساب کاربران به نقش‌ها با توجه به شیفت‌های کاری در بخش‌های سازمان و حمایت از