طبقه‌بندی وظایف در کنترل کاربرد

کامیار رفعتی ۸۴۲۰۳۶۹۴
rafati@ce.sharif.edu
دانشکده‌ی مهندسی کامپیوتر
دانشگاه صنعتی شریف

نعیم اصفهانی ۸۴۲۰۱۰۰۳
esfahani@ce.sharif.edu
دانشکده‌ی مهندسی کامپیوتر
دانشگاه صنعتی شریف

درس سیستم عامل‌های پیشرفته
مدرس: دکتر جلیلی

کلمات کلیدی:
مدل امنیتی، کنترل کاربرد، وظیفه‌ها

چکیده:

موضوعات کنترل دسترسی[1] و مدیریت اعتماد[2] و مدیریت حقوق الکترونیکی[3] موضوعات بحث برانگیزی در امنیت سیستم‌ها هستند. در کنترل دسترسی بررسی می‌کنیم که هر کاربری به چه منابعی دسترسی دارد. موضوع مبحث مدیریت اعتماد، اعطای دسترسی به کاربران ناشناس در یک محیط باز مثل اینترنت می‌باشد و در نهایت مدیریت حقوق الکترونیکی عبارت است از کنترل دسترسی و استفاده از اشیاء الکترونیکی بعد از انتشار آن‌ها (انتقال آن‌ها به کاربر).

امروزه با توجه به پیشرفت‌های صورت گرفته در زمینه‌ی تکنولوژی اطلاعات و تاثیرات اجتماعی آن‌ها، مدل‌های قدیمی امنیت دیگر پاسخگو نیستند؛ مدل‌های قدیمی عمدتا در محیط‌های بسته عمل می‌کردند. ویژگی این محیط‌ها وجود کاربران مشخص و نظارت متمرکز می‌باشد، این در حالی است که نیازهای جدید عمدتا در محیط‌های باز مطرح می‌شوند که کاربران ناشناخته با قوانین شناسایی پویا دارند. این نیازمندی‌های جدید، مسائل امنیتی را برمی‌انگیزد که نیازمند عناصری از هر سه مبحث مطرح شده، می‌باشند. *کنترل کاربرد*[4] با متحد کردن مباحث کنترل دسترسی، مدیریت اعتماد و مدیریت حقوق الکترونیکی، در یک سیستم مجتمع، نسل جدیدی از مدل‌های امنیت در سیستم‌ها را معرفی کرده‌است. هدف از این تحقیق بررسی مدل کنترل کاربرد و ارائه‌ی طبقه بندی برای یکی از اجزای آن به نام وظیفه‌ها می‌باشد.

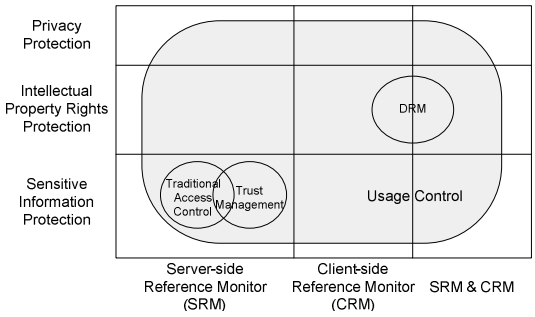
[1] Access Control
[2] Trust Management
[3] Digital Right Management
[4] Usage Control

۱- مقدمه:

پیشرفت‌های انجام شده در حوزه‌ی فناوری اطلاعات و شبکه امکان دسترسی و استفاده‌ی فراگیر[5] از اطلاعات دیجیتال باعث تحول شگرفی در نوع و مدل زندگی انسان‌ها گشته است. به دلیل این نوآوری‌ها دیگر اطلاعات محدود به ماندن درون رایانه‌ها نیستند بلکه می‌توان آن‌ها را بر روی بسیاری از دستگاه‌های دیگر از جمله دستگاه‌های سیار (پخش کننده‌های موسیقی، تلفن‌های همراه، کامپیوترهای دستی و ...)، دستگاه‌های خانگی متصل به شبکه‌ی جهانی (ضبط صوت، سیستم تهویه و ...) نیز دید. این دستگاه‌ها می‌توانند با روش‌های ارتباطی مختلفی به هم متصل شوند و این باعث به وجود آمدن محیط محاسباتی فراگیر شده‌است؛ این محیط فراگیر چالش‌های جدیدی را در راستای کنترل بر روی استفاده از اطلاعات دیجیتال در زمان حیاتشان به وجود آورده است، به گونه‌ای که روش‌های سنتی موجود، دیگر جوابگوی نیازهای مطرح شده در این محیط فراگیر نیستند و نیاز به روش‌های نوین احساس می‌شود.

مدل‌های مختلفی در زمینه‌ی کنترل دسترسی مطرح شده‌اند که به طور مثال می‌توان به کنترل دسترسی اجباری[6] (MAC)، کنترل دسترسی بصیرتی[7] (DAC) و کنترل دسترسی برپایه‌ی نقش[8] (RBAC) اشاره کرد. این مدل‌ها خود را متمرکز بر محیط‌های بسته نموده‌اند و همچنین ساختاری ایستا دارند بنابراین توان پوشش محیط‌های الکترونیکی باز امروزی را ندارند و همچنین امکان اعتبار سنجی پویا را ندارند. بعلاوه این مدل‌ها فقط کاربران شناخته شده را مورد پوشش قرار می‌دهند که مناسب محیط‌های گسترده‌ی امروزی مانند اینترنت نیست.

در مدیریت اعتماد سعی در رفع مشکل شناخته نبودن



شکل ۱: پوشش مدل‌های مختلف

به وجود آوردن امکان محافظت از حق مالکیت معنوی دارد، مدل‌های دیگری نیز برای مشکلات مطرح دیگر معرفی شده‌اند که از این جمله‌اند کنترل دسترسی بر پایه‌ی کار[9] (TBAC) و کنترل دسترسی بر پایه‌ی شرایط[10] (PBAC). همان طور که در شکل مشاهده می‌شود برای بحث محافظت از حریم خصوصی کاربران حتی مدلی ارائه نشده، در حقیقت بسیاری از قسمت‌های موجود در گستره‌ی سیستم‌ها توسط مدل‌های موجود پوشش داده نمی‌شوند و مدل‌های موجود هرکدام جنبه‌ای از سیستم را مورد پوشش قرار می‌دهند. در این میان نیاز به مدلی یک‌پارچه که توانایی پوشش تمام نیازهای جدید و به تبع آن سیستم‌های جدید را داشته باشد، مشهود است. اخیرا چنین مدلی با نام کنترل کاربرد توسط آقای پارک و سندهو [1, 3, 6] معرفی شده‌است.

مدل مطرح شده بسیار جوان است و بیشتر کارهای انجام شده روی آن در راستای معرفی و نشان دادن قدرت آن در برابر مدل‌های سنتی بوده است و در نهایت برای این مدل منطقی معرفی شده است تا بتوان مفاهیم امنیتی را به صورت گزاره‌هایی بیان کرد. در این میان با توجه به نو بودن مدل هنوز عناصر پایه‌ای مدل مورد بررسی دقیق و طبقه‌بندی قرار نگرفته‌اند. بدیهی است که قبل از هرگونه کار عملی و پیاده‌سازی باید جنبه‌های مختلف مدل بررسی و طبقه‌بندی شوند.

---

[5] Pervasive
[6] Mandatory Access Control
[7] Discretionary Access Control
[8] Role-Based Access Control

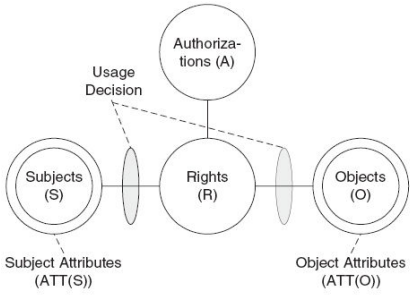
[9] Task-Based Access Control
[10] Provision-Based Access Control

در این مقاله طبقه‌بندی یکی از عناصر پایه‌ای مدل کنترل کاربرد به نام وظیفه‌ها را خواهیم دید بعلاوه بررسی کوچکی در مورد یکی دیگر از عناصر پایه‌ای به نام شرط‌ها را خواهیم داشت.

در ادامه ابتدا در بخش ۲ معرفی مختصری از مدل کنترل کاربرد خواهیم داشت. در بخش ۳ طبقه‌بندی وظیفه‌ها را انجام می‌دهیم و در بخش ۴ گسترش کوچکی به مدل در قسمت شرط‌ها داده می‌شود.

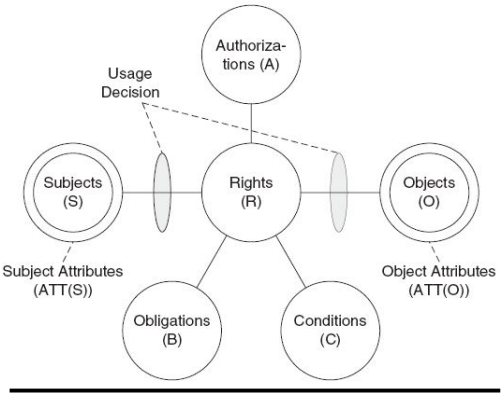
۲- مدل کنترل کاربرد:

وجه مشترک روش‌های سنتی کنترل دسترسی و همچنین مدیریت اعتماد، استفاده از صفات کاربران[11] و منابع[12] مورد دسترسی برای اعتبار سنجی[13] می‌باشد. به بیان دیگر در روش‌های سنتی تصمیم در مورد معتبر بودن بر مبنای صفات کاربر و صفات منبع مورد دسترسی و حقوق[14] مورد نیاز اتخاذ می‌شود. در این‌جا اعتبار سنجی در حقیقت شامل گزاره‌هایی وابسته به اعضاست که برای تصمیم‌گیری در مورد اجازه‌ی استفاده از یک منبع ارزیابی می شوند و حق شامل امتیاز یک کاربر بر روی یک منبع می‌باشد.



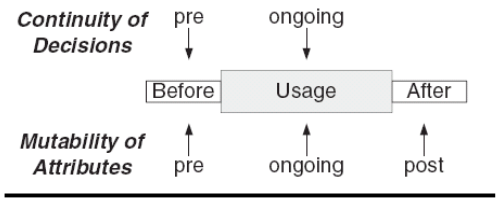
شکل ۲: مدل‌های کنترل دسترسی سنتی

[11] Subjects
[12] Objects
[13] Authorization
[14] Rights



شکل ۳: مدل کنترل کاربرد

در مدل کنترل کاربرد دو مفهوم کلیدی جدید به روش‌های سنتی اضافه شده است؛ این مفاهیم عبارتند از وظیفه‌ها[15] و شرط‌ها[16]. به مجموعه‌ی کارهای مشخصی که کاربر باید انجام دهد تا بتواند از یک منبع استفاده نماید وظیفه می‌گویند. و به عبارت دیگر وظیفه‌ها شامل گزاره هایی که وظایف فرد را قبل و حین دسترسی مشخص می کنند هستند. شرط‌ها شامل فاکتورهایی در تصمیم‌گیری هستند که از محیط و سیستم نشات می‌گیرند و به صورت گزاره هایی که وضعیت محیط یا سیستم را در هنگام دسترسی ارزیابی می کنند بیان می‌شوند. شایان ذکر است که در مدل کنترل کاربرد شرط‌ها امکان تغییر صفات را ندارند.



شکل ۴: استمرار و تغییر پذیری صفات

مدل کنترل کاربرد علاوه بر سه فاکتور اجازه، وظیفه و شرط که در تصمیم‌گیری موثر هستند، دو مفهوم استمرار و تغییرپذیری را نیز معرفی نموده است. استمرار به معنی پیوستگی در انجام فرایند

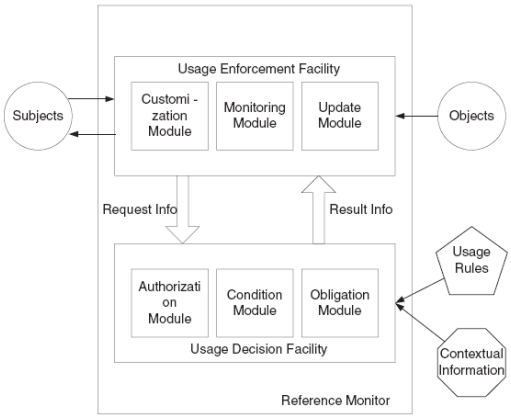
[15] Obligations
[16] Conditions

اعتبارسنجی - حتی در حین دسترسی – است؛ با توجه به این عامل مشخص می‌شود که در چه مواقعی (قبل عمل ویا حین عمل) می‌توان یک صفت را تغییر داد. تغییرپذیری مشخص کننده‌ی امکان تغییر صفات کاربر و یا منبع در اثر دنباله‌ای مشخص از دسترسی‌هاست زمان تغییر صفت (قبل عمل، حین عمل ویا بعد از عمل) نیز مشخص می‌شود. با بیان چند مثال ساده برای فهم بهتر مدل این بخش را به پایان می‌بریم:

- در تلفن راه دور که توسط خط تلفن انجام می‌گیرد اعتبار سنجی در ابتدا انجام شده، شرکت مخابرات توسط سیم به تلفن مشتری وصل است و مطمئن است که تنها او می‌تواند شماره‌گیری کند. به روز رسانی صفات او نیز در انتها صورت می‌گیرد، این تماس و زمان آن به لیست مکالمات مشتری اضافه می‌شود.
- در مورد تلفن کارتی هردوی این امور در حین دسترسی اتفاق می‌افتد؛ اعتبار سنجی با حضور کارت انجام می‌شود و هزینه‌ی مکالمه به صورت درجا از اعتبار کارت که یکی از صفات است کاسته می‌شود و آن صفت را تغییر می‌دهد.
- با روز خرید غذا شما عملا اعتبار سنجی و به روز رسانی را در ابتدا انجام می‌دهید. در ابتدا با توجه بودن غذای اضافه و اجازه‌ی خرید اعتبار سنجی شده و سپس با تهیه‌ی ژتون به روز رسانی انجام می‌شود؛ هردوی این اعمال در ابتدا اتفاق می‌افتند.
- وقتی به سایتی مراجعه می‌کنید که باید هر ۴۰ ثانیه روی یک آگهی کلیک کنید تا مطالب را بخوانید عملا وظیفه‌ی شما کلیک کردن است و آن را باید در حین دسترسی انجام دهید، این عمل باعث به‌روز شدن یک صفت (شمارنده) با هر کلیک در حین دسترسی می‌شود.
- ساعت کاری یک اداره یا یک سیستم مشخص کننده‌ی شرط‌ها در ابتدا و در حین دسترسی یا استفاده از سرویس‌های سیستم می‌باشد.

مانند هر سیستم دیگری در این سیستم نیز برای اعمال سیاست‌های اتخاذ شده نیاز به یک ناظر مرجع وجود دارد. استانداردهای گوناگونی برای معماری ناظر وجود دارد که معروف‌ترین آن توسط سازمان ISO طراحی شده است و با استاندارد [ISO/IEC 10181-3] ارائه شده است. در تمام این استانداردها دو قسمت اساسی ثابت است. اول بخش انجام و اعمال کنترل دسترسی است که وظیفه اعمال تصمیمات گرفته شده را بر عهده دارد. بخش دم ، بخش اتخاذ تصمیمات است که وظیفه آن تصمیم‌گیری در مورد استفاده یک متقاضی از یک منبع می‌باشد. نکته مهم در مورد ناظر مرجع این است که اولاً همیشه باید حضور داشته باشد و ثانیاً هرگز نباید بتوان از کنار آن گذشت.

مرجع پیشنهادی در مدل کنترل کاربرد همانند مدل استاندارد است ولی جزئیات آن اندکی متفاوت است که در ادامه در مورد آن صحبت می‌کنیم. شکل ۵ مرجع پیشنهاد شده در مدل کنترل کاربرد را نشان می‌دهد.



شکل ۵: مدل ناظر مرجع

در مدل فوق دو قسمت اصلی امکان اعمال کاربرد و امکان تصمیم‌گیری کاربرد وجود دارند که همانند آنچه در مدل‌های استاندارد گفته شد عمل می‌نمایند. تفاوت در جزئیات سازنده این قسمت‌ها می‌باشد. در قسمت تصمیم‌گیری کاربرد از اجزا کنترل شرایط و کنترل وظایف به همراه قسمت ایجاد مجوز تشکیل شده است.

در قسمت ایجاد مجوز ، مانند مدل‌های سنتی کنترل دسترسی ، بر مبنای صفات متقاضی و شی مورد دسترسی و همچنین قوانین موجود ، تصمیمی مبنی بر اعطای مجوز و یا جلوگیری از دسترسی گرفته می‌شود و به قسمت اعمال کنترل فرستاده می‌شود. ممکن است اطلاعاتی دالّ بر چگونگی آماده کردن[17] شی برای استفاده نیز فرستاده شود. واحد کنترل شرایط نیز به کمک قوانین و شرایط محیطی مجوز مربوطه را صادر می‌نماید. واحد کنترل وظایف علاوه بر کنترل پیش-شرط‌های استفاده ، شروط زمان اجرا و پس‌شرط‌ها را بررسی می‌نماید. قسمت اعمال کاربرد نیز از بخش‌های آماده‌سازی ، نظارت و به روز کردن صفات تشکیل شده است. در قسمت آماده‌سازی شی مورد دسترسی با استفاده از اطلاعات واحد ایجاد مجوز برای استفاده متقاضی آماده می‌شود. در قسمت به روز کردن صفات نیز با توجه به تقاضاها و دسترسی‌های متقاضیان ، صفات هر متقاضی و یا شی به روز می‌شود.

با توجه به اینکه ناظر مرجع در سمت سرویس‌دهنده باشد و یا در سمت سرویس‌گیرنده ، معماری‌های گوناگونی وجود دارد. در معماری نوع اول ، ناظر مرجع در سمت سرویس‌دهنده است و لذا از قابلیت اطمینان بیشتری برخوردار است. در نوع دوم معماری ، ناظر تماما در سمت سرویس‌گیرنده است ، با وجود اینکه این روش قابلیت اطمینان کمتری نسبت به روش اول برخوردار است ولی به علت وجود انعطاف‌پذیری بیشتر همچنان مورد توجه است. این معماری امکان اعمال کنترل حتی بعد از واگذار کردن شی به متقاضی را دارد. مدل سوم تلفیقی از مدل‌های اول و دوم است به گونه‌ای که بخشی از ناظر در سمت سرویس‌دهنده و بخشی در سمت سرویس‌گیرنده قرار دارد. این مدل مزایا هر دو مدل اول را دارد ولی از پیچیدگی نسبتا زیادی برخوردار است.

[17] customization

۳- دسته بندی وظایف:

یکی از عناصر هسته مدل کنترل کاربرد وظایف می-باشد. وظایف یکی از نقاط قوت این مدل است که آن را از مدل‌های سنتی متمایز می‌کند و برای کاربردهای جدید مناسب می‌نماید. به دلیل تازگی و بدیع بودن این عنصر تاکنون بحث زیادی در مورد انواع آن و چگونگی پیاده‌سازی و اعمال آنها در ادبیات این شاخه از علم وجود ندارد. به منظور عملی شدن استفاده از مفهوم وظیفه در این بخش به بیان برخی از دسته-بندی‌های ممکن از این عنصر ، که می‌تواند در پیاده-سازی آن کمک کند ، می‌پردازیم.

اولین دسته بندی بر مبنای مدت زمان اجرای یک وظیفه است. بر این مبنا وظایف به دو دسته مدت ثابت و نامحدود تقسیم می‌شوند. باز بودن یک تبلیغ در طول مدت استفاده از یک وب سایت از نوع وظایف مدت ثابت است ولی انتشار یک کتاب الکترونیکی بعد از دریافت از سایت ، از نوع نامحدود است زیرا هیچ وقت نباید در اختیار دیگران قرار گیرد.

قابلیت مشاهده ناظر ، یکی از معیارهایی است که می-توان به کمک آن این تقسیم بندی را انجام داد. پرداخت مبلغ یک کالای الکترونیکی قبل از استفاده از آن از جمله وظایف قابل مشاهده برای ناظر است ولی در مقابل اینکه یک شیئ الکترونیکی باید ظرف یک بازه محدود زمانی پاک شود برای ناظر قابل مشاهده نیست.

تلفیق دسته بندی های فوق می‌تواند حالت‌هایی تولید کند که همه آنها قابل تصور هستند.(جدول۱)

	قابل مشاهده	غیر قابل مشاهده
مدت ثابت	✓	✓
نامحدود	✓	✓

جدول ۱: حالات تلفیق دسته‌بندی‌ها

از نظر زمان اجرای یک وظیفه می‌توان وظایف را به سه دسته تقسیم نمود. دسته اول قبل از انجام دسترسی بررسی می‌شوند مانند پرداخت مبلغ یک کلاس الکترونیکی قبل از استفاده از آن. در دسته دوم وظایف در حین دسترسی بررسی می‌شوند مانند باز بودن یک تبلیغ هنگام استفاده از امکانات وب سایت. دسته آخر که وظایفی هستند که بعد از انجام دسترسی بررسی می‌شوند از مابقی دشوارتر به نظر می‌رسند مانند خرید به صورت اقساط کوتاه و یا بلند مدت.

یکی از معیارهای مناسب در عمل ، نوع منطق گزاره‌ای وظیفه است. وظایفی که منطق منفی دارند بهتر به کمک توابع ماشه‌ای[18] قابل پیاده‌سازی هستند. از جمله آنها ، عدم نسخه‌های رونوشت از یک فایل است. در مقابل آنهایی هستند که منطقی مثبت دارند.

وظایف ممکن است توانایی تغییر صفات را داشته باشند مثلا استفاده از یک موسیقی به صورت خرید دقیقه‌ای که در آن به ازای هر دقیقه استفاده از موسیقی مبلغ معینی از حساب شخص کم می‌شود. همچنین ممکن است که توانایی تغییر صفات را نداشته باشد.

وظایف مبتنی بر تاریخ وظایفی هستند که سوابق گذشته فرد در آنها تاثیر دارد مانند اینکه قبل از استفاده از امکانات سایت ، حتما باید مراحلی انجام شود. در مقابل وظایفی هستند که به گذشته مربوط نیستند مانند مثال موسیقی. پس تاریخ نیز می‌تواند یک معیار مناسب برای دسته بندی باشد.

آخرین دسته بندی که بر مبنای حساسیت به محیط است ، وظایف را به دو دسته تقسیم می‌نماید. دسته اول وظایف حساس به محیط هستند. مثلا استفاده از امکانات سایت در ساعت‌های پر ترافیک گران‌تر از ساعات کم ترافیک است. دسته دوم نیز آنهایی هستند که به محیط حساس نیستند که اکثر مثال‌های آورده شده در این بخش از این دسته هستند.

در این بخش دسته بندی‌های گوناگونی از وظایف را دیدیم. این دسته بندی‌ها می‌تواند کمک شایانی به نزدیک شدن این مفاهیم ، عمدتا تئوریک ، به مباحث مطرح در پیاده‌سازی نماید.

۴- شرایط تاثیرگذار:

در این بخش ابتدا مثال‌هایی را با هم می‌بینیم که مدل کنترل کاربرد که توسط آقای پارک و همکارشان [1] مطرح شده است قابل بیان نیستند. سپس علت عدم توانایی این مدل را در بیان این مثال‌ها بررسی می‌کنیم و در نهایت راهکاری برای آن ارائه می دهیم.

مثال ۱ : ثبت کاربرانی که در زمان حمله از سیستم استفاده می کنند به عنوان مخاصم احتمالی – در یک سیستم مدیران تصمیم می‌گیرند که به منظور کاهش خطر حمله به سیستم ، کاربرانی را که در زمان یک حمله به سیستم در سیستم مشغول به کار هستند را به عنوان مخاصم احتمالی ثبت نمایند و میزان اعتماد به آنها را کاهش دهند تا در صورت تکرار این امر ، آنها را اخراج نمایند.

مثال ۲ : تعداد دسترسی های همزمان به یک شیئ در شرایط مختلف سیستم – مدیران تصمیم می‌گیرند تا در زمان‌های پر ترافیک برای سیستم ، اجازه دسترسی همزمان به اشیا مختلف را کاهش دهند و همچنین زمان‌های کم ترافیک این مقدار را افزایش دهند. اگر این مقدار برای اشیا مختلف یکسان باشد مشکلی وجود ندارد ولی در شرایطی که این مقدار برای اشیا مختلف یکسان نباشد این مدل دچار مشکل می-شود.

مثال ۳ : اعطای حقوق ویژه دائمی به کسانی که در یک زمان خاص از سیستم استفاده نموده اند – این تصمیم گرفته می‌شود که افرادی که در روز افتتاح سیستم به آن مراجعه نمایند برای همیشه به عنوان مهمان ویژه شناخته شوند.

همانطور که گفته شد مدل اصلی کنترل کاربرد در بیان مثال‌های فوق دچار مشکل می‌شود و به سادگی نمی-

[18] Trigger

توان آنها را بیان نمود. خاصیت مشترکی که در تمام مثال‌های فوق دیده می‌شود این است که برخی از شرایط محیطی باعث ایجاد تغییر در صفات یک شیئ و یا یک فرد متقاضی می‌شود. مثلا در مثال اول شرایط حمله در محیط باعث کاهش میزان اعتماد یک شخص می‌شود. در مدل اصلی کنترل کاربرد که آقای پارک و همکارشان [1] ارائه داده‌اند ، این نکته به صورت صریح گفته شده است که شرایط محیطی نمی‌توانند صفات اشیا و افراد را تغییر دهند. به نظر می‌رسد که اضافه کردن قابلیت تغییر صفات افراد و اشیا در ازای شرایط خاص محیطی می‌تواند این مشکلات را حل نماید.

۵- نتیجه‌گیری:

در این مقاله مروری بر روی نیازمندی‌های جدید امنیت و نارسایی‌های مدل‌های موجود در کنترل دسترسی انجام داده شد، در ادامه معرفی مختصری از مدل کنترل کاربرد به عنوان راه حلی بر این مشکلات ارائه شد. سپس به منظور پیش‌برد مدل و روشن شدن مفهوم وظایف و کمک به نزدیک کردن تئوری به پیاده‌سازی ، طبقه بندی‌های مختلفی برای آن ارائه شده است. در نهایت با بررسی چند مثال ، محدودیت احتمالی مدل کنترل کاربرد نشان داده شده و راه‌کاری برای آن ارائه شد.

۶- منابع:

[1] Park, J. and Sandhu, R. *Towards usage control models: beyond traditional access control*, In Proceedings of the Seventh ACM Symposium on Access Control Models and Technologies (Monterey, California, USA, June 03 - 04, 2002), SACMAT '02, ACM Press, New York, NY, 57-64.

[2] Hilty, M., Basin, D., Pretschner, A, *On Obligations* Proc 10th European Symp on Research in Computer Security (ESORICS'05), Springer LNCS 3679, pp. 98-117, Milan, Sep. 2005.

[3] Park, J. and Sandhu, R, *the UCONABC usage control model*, ACM Trans Inf Syst Secur 7, 1 (Feb. 2004), 128-174.

[4] Zhang, X., Park, J., Parisi-Presicce, F., and Sandhu, R, *A logical specification for usage control*, In Proceedings of the Ninth ACM Symposium on Access Control Models and Technologies (Yorktown Heights, New York, USA, June 02 - 04, 2004), SACMAT '04. ACM Press, New York, NY, 1-10.

[5] Jagadeesan, R. and Marrero, W, *Timed constraint programming: a declarative approach to usage control*, In Proceedings of the 7th ACM SIGPLAN international Conference on Principles and Practice of Declarative Programming (Lisbon, Portugal, July 11 - 13, 2005), PPDP '05. ACM Press, New York, NY, 164-175.

[6] R. Sandhu and J. Park, *Usage Control: A Vision for Next Generation Access Control*, the Second International Workshop on Mathematical Methods, Models and Architectures for Computer Networks Security, 2003.

[7] Jaehong Park, Xinwen Zhang, and Ravi Sandhu, *Attribute Mutability in Usage Control*, 18th Annual IFIP WG 11.3 Working Conference on Data and Applications Security, 2004.