چهارمین کنفرانس انجمن رمز ایران
۲۴ الی ۲۶ مهر ماه ۱۳۸۶ دانشگاه علم و صنعت ایران
انجمن رمز ایران
Iranian Society of Cryptology
Archive of SID

توصیف و استنتاج خط‌مشی‌های دسترسی و الزام بر مبنای منطق هنجارها در محیط‌های آگاه از معنا

مرتضی امینی
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف
m_amini@ce.sharif.edu

رسول جلیلی
دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف
jalili@sharif.edu

چکیده: ظهور تکنولوژی معنایی در طی سال‌های اخیر و به دنبال آن پیدایش محیط‌های آگاه از معنا، راه را برای هوشمندی ماشین‌ها در تفسیر و پردازش اطلاعات و تعامل بیشتر با یکدیگر هموار نموده است. خصوصیات ویژه محیط‌های آگاه از معنا، نیازمندی‌های امنیتی خاصی را به خصوص در مجازشماری تحمیل می‌نماید. یک مدل مناسب برای محیط‌های آگاه از معنا باید نیازمندی‌هایی همچون کنترل استنتاج بر اساس روابط معنایی در دامنه‌های مختلف عامل‌ها، اشیا، و اَعمال، آگاهی از زمینه، برخورداری از معنایی صریح و دقیق، رفع تداخل، توصیف و مدیریت توزیع‌شده خط‌مشی را پوشش دهد. نیاز به یک مدل امنیتی مبتنی بر نیازمندی‌های مطروحه، حاوی ساختار نحوی، معناشناسی و قابلیت استنتاج ما را به سمت استفاده از منطق در مدل امنیتی برای محیط‌های آگاه از معنا سوق می‌دهد. بر این اساس در این مقاله نسخه اولیه یک مدل آگاه از معنا مبتنی بر ترکیبی از منطق هنجارها و منطق توصیفی پیشنهاد می‌گردد. به‌کارگیری منطق هنجارها در این مدل، امکان توصیف خط‌مشی‌های کنترل دسترسی را در کنار خط‌مشی‌های الزام فراهم می‌نماید و لذا مساله تداخل بین این دودسته خط‌مشی را نیز تحت کنترل در می‌آورد.

واژه‌های کلیدی: مدل امنیتی، کنترل دسترسی، منطق هنجارها، کنترل دسترسی مبتنی بر منطق

۱- مقدمه

گسترش استفاده از سیستم‌های کامپیوتری و پردازش‌های ماشینی از یک سو و مهارت رو به رشد مهاجمان سیستم‌ها و شبکه‌های کامپیوتری از سوی دیگر نگرانی رو به رشدی را به دنبال داشته است. تبدیل دارایی‌های فیزیکی به دارایی‌های الکترونیکی و جایگزینی امور دستی با امور ماشینی، نیازمندی‌های حفاظتی و امنیتی را در جوامع انسانی از حفاظت فیزیکی به حفاظت از دارایی‌ها و رویه‌ها در فضای تبادل اطلاعات تغییر داده است.

مشکل اصلی فضای تبادل اطلاعات، عدم وجود مرزهای مشخصی است که در فضای فیزیکی موجود است. این ابهام در مرزها وقتی بیشتر جلوه می‌کند که بخواهیم امکان محاسبات توزیع‌شده و فراگیر[1] را در یک محیط آگاه از معنا فراهم نماییم.

[1] Pervasive Computing

www.SID.ir

Archive of SID

در واقع در این محیط‌های محاسباتی جدید، می‌خواهیم منابع پردازشی و اطلاعاتی خود را به امید دستیابی به قدرتی بیشتر به اشتراک گذارده، با افزایش سطح تعاملات ماشین‌ها از بار محاسباتی انسان‌ها بکاهیم. حال مساله این است، چگونه باید امنیت فضای الکترونیکی خود را حفظ نماییم و چگونه دسترسی افراد و ماشین‌ها را به منابع پردازشی و اطلاعاتی خود کنترل نماییم.

شکل‌گیری محیط‌های آگاه از معنا، نیازمندی‌های امنیتی جدید و خط‌مشی‌های جدیدی را به دنبال داشته است که قطعاً با مدل‌های امنیتی و مجازشماری قدیمی قابل ارضاء نبوده است. برای این منظور تلاش‌های متعددی در خصوص ارائه مدل و یا ارائه مکانیزم‌های کنترل دسترسی مناسب صورت پذیرفت. نقطه ضعف اغلب کارهای تحقیقاتی انجام شده، عدم نیازسنجی امنیتی برای محیط‌های آگاه از معنا بوده است. همین امر منجر به ارائه مدل‌های ناقص و ناکارآمدی گردید که بخشی از نیازها را پوشش نمی‌دادند. از مهم‌ترین نیازهایی که موردغفلت واقع شد، نیاز به کنترل استنتاج است. وجود این نوع کنترل با در نظر گرفتن روابط معنایی بین عامل‌ها، اشیاء و اَعمال، نیاز به استقلال مدل از پیاده‌سازی (با توجه به نامتجانس بودن سیستم‌ها) و امکان اِعمال خط‌مشی‌های امنیتی در سطوح مختلف با ریزدانگی متفاوت، امری ضروری به نظر می‌رسد.

مبتنی بودن محیط‌های آگاه از معنا بر پایه منطق (و به طور خاص منطق توصیفی[۲] [۱])، نیاز به استنتاج در مدل مجازشماری این محیط‌ها، برخورداری از معنا در خود مدل و نیاز به استقلال از پیاده‌سازی، ما را بر آن داشت که به سوی ارائه یک مدل مبتنی بر منطق برای این محیط محاسباتی جدید روی آوریم.

مبنای راه‌حل پیشنهادی در این مقاله منطق هنجارها[۳] است که گونه خاصی از منطق موجهات[۴] است و خاستگاه اصلی آن علم حقوق و اخلاق است. قبل از این نیز، از منطق هنجارها در مجازشماری استفاده شده است ولی آنچه که ما به دنبال آن هستیم، ترکیب آن با منطق توصیفی به لحاظ نحوی و معنایی برای شکل‌گیری یک مدل امنیتی با قابلیت استنتاج و امکان بیان خصوصیات ایمنی[۵] و بقاء[۶] در محیط‌های آگاه از معنا است.

براین اساس در ادامه در بخش ۲ به کارهای انجام شده در زمینه کنترل دسترسی در محیط‌های آگاه از معنا و همچنین مرور مدل‌های امنیتی و کنترل دسترسی مبتنی بر منطق خواهیم پرداخت. در بخش ۳ پس از ارائه برخی مطالب پیش‌نیاز، به معرفی مولفه‌های اصلی مدل پیشنهادی پرداخته خواهد شد. بخش ٤ به ارائه ساختار نحوی، نظریه برهان (شامل اصول موضوعه و قواعد استنتاج) و معناشناسی منطق توصیف خط‌مشی‌های امنیتی می‌پردازد. بخش ۵ مولفه‌های فراخط‌مشی مدل و اَعمال مدیریتی مورد نیاز در آن را بیان می‌نماید. در بخش ٦ به ارائه یک مثال از کاربرد مدل پیشنهادی پرداخته خواهد شد و نهایتاً بخش ۷ به جمع‌بندی و ترسیم مسیر آتی این پژوهش خواهد پرداخت.

۲- کارهای انجام شده

با ظهور تکنولوژی معنایی و شکل‌گیری محیط‌های آگاه از معنا مانند وِب‌معنایی مباحث متعددی بر روی نحوه فراهم‌سازی امنیت برای اینگونه محیط‌ها شکل گرفت. بوناتی و همکارانش در [۲] به طرح نیازمندی‌ها و بسیاری از مسائل باز تحقیقاتی در این زمینه و به خصوص کنترل دسترسی پرداخته‌اند.

یکی از زبان‌های معروف ارائه شده برای بیان خط‌مشی‌های امنیتی در وِب‌معنایی توسط کاگال و فینین [۳] ارائه شده است. این زبان بر اساس دو زبان بیان آنتالوژی RDF و DAML+OIL بیان شده است و امکان توصیف مجوزها، ممنوعیت‌ها و الزام‌ها را با الهام از منطق هنجارها فراهم می‌آورد. مشکل عمده این زبان و چارچوب ارائه شده برای آن با نام Rein، عدم در نظر گرفتن تاثیر روابط معنایی بر انتشار حقوق دسترسی است. کوئین و همکارانش [۴] نیز یک مدل کنترل دسترسی سطح مفهوم ارائه نموده‌اند که تاثیر روابط معنایی بین اشیاء را در کنترل دسترسی در نظر گرفته‌اند. وجود ناسازگاری در قواعد انتشار ارائه شده برای انواع مختلف روابط

[2] Description Logic
[3] Deontic Logic
[4] Modal Logic
[5] Safety
[6] Liveness

www.SID.ir

باعث ناکارآمدی این مدل شده است. در ادامه این روند، یک مدل کنترل دسترسی با نام SBAC توسط جوانمردی و همکارانش در [۵] ارائه گردید که امکان کنترل انواع کانال‌های استنتاج را در سه حوزه عامل‌ها، اشیاء و اَعمال فراهم می‌نمود. در این مدل همه روابط معنایی به یک رابطه، آن هم رابطه شمول[۷] تبدیل می‌شود و سپس تاثیر رابطه شمول بر انتشار قواعد دسترسی مثبت و منفی در هر سه حوزه عامل‌ها، اشیاء و اَعمال به صورت چند قاعده ساده ارائه می‌گردد.

استفاده از منطق در کنترل دسترسی و مجازشماری، از سال ۱۹۹۸ توسط گلاسگو [۶] آغاز گردید. از آن زمان تاکنون انواع مختلفی از منطق از جمله منطق مرتبه اول، منطق لایه‌لایه[۸]، و انواع منطق موجهات (شامل منطق زمانی[۹]، منطق شناخت[۱۰] و منطق هنجارها) برای توصیف انواع خط‌مشی‌ها و محدودیت‌های زمینه‌ای و زمانی حاکم برآنها و همچنین وارسی امنیتی در محیط‌های محاسباتی توزیع شده استفاده شده است. آنچه که موجب استفاده از منطق در کنترل دسترسی شده است، عدم وجود ابهام در منطق و برخورداری از معناشناسی و قدرت بیان مطلوب و مهم‌تر از همه داشتن سطح انتزاعی مناسب برای بیان انواع خط‌مشی‌ها، مستقل از زیرساخت و نحوه پیاده‌سازی است.

منطق ارائه شده توسط آبادی، لمپسون و همکارانش [۷] برای توصیف عامل‌های مرکب در محیط‌های توزیع شده و ارائه یک مدل مبتنی بر منطق موجهات بر اساس لیست کنترل دسترسی، از کارهای برجسته در زمینه به‌کارگیری منطق در کنترل دسترسی به شمار می‌آید. وُو و لَم [۸] نیز برای اولین یک چارچوب منطقی عمومی برای کنترل دسترسی در محیط‌های توزیع‌شده بر مبنای منطق پیش‌فرض (که نوعی منطق غیریکنوا[۱۱] به شمار می‌رود) ارائه نموده‌اند. تصمیم‌ناپذیری منطق ارائه شده توسط این دو محقق، جاجودیا و همکارانش را به تدوین یک زبان مبتنی بر منطق مرتبه اول لایه‌لایه با نام ASL [۹] ترغیب نمود. زبان ASL امکان بیان قواعد استنتاج، قواعد رفع تداخل، قواعد رفع تداخل، قواعد جامعیتی و تغییر قواعد تصمیم‌گیری در خصوص دسترسی را فراهم می‌آورد. بدین ترتیب این زبان قادر به بیان انواع مختلفی از خط‌مشی‌ها از جمله خط‌مشی دیوار چینی و خط‌مشی تفکیک وظایف پویا می‌باشد.

استفاده از منطق زمانی نیز برای توسعه مدل نقش‌مبنای RBAC مورد توجه جوشی و همکارانش بوده است که حاصل آن ارائه مدل GTRBAC [۱۰] می‌باشد، که امکان توصیف محدودیت‌های زمانی و دوره‌ای بر روی انتساب نقش‌ها به کاربران و انتساب مجوزها به نقش‌ها را فراهم می‌آورد. تلاشهای انجام شده توسط کوپنز و همکارانش بین سالهای ۱۹۹۰ تا ۱۹۹۶ [۱۱-۱۳] در به کارگیری منطق هنجارها در ترکیب با سایر منطق‌ها از جمله منطق شناختی و منطق زمانی برای کنترل جریان اطلاعات (کنترل آنچه که کاربر مجاز است بداند) قابل توجه است.

آنچه که در این نوشتار مورد توجه است، به کارگیری منطق هنجارها در ترکیب با منطق توصیفی برای کنترل دسترسی و کنترل انواع کانال‌های استنتاج با بهره‌گیری از قدرت استنتاج این دو منطق می‌باشد. بدین‌ترتیب ضعف موجود در بسیاری از مدل‌های ارائه شده در کنترل دسترسی محیط‌های آگاه از معنا (یعنی عدم تاثیرگذاری روابط معنایی بر انتشار قواعد امنیتی و دسترسی) با بهره‌گیری از منطق مرتفع گردیده است.

۳- مدل امنیتی مبتنی بر منطق هنجارها

مدل ارائه شده در این مقاله مشابه معماری ارائه شده در [۱۴] بر این فرض استوار است که یک محیط آگاه از معنا به چند دامنه تقسیم می‌شود که هر دامنه شامل تعدادی شیئ می‌باشد که خود را در آن ثبت نموده‌اند. هر دامنه دارای یک مدیر امنیتی است که مجموعه قواعد امنیتی و دسترسی حاکم بر اشیاء موجود در آن دامنه را تدوین و اِعمال می‌نماید. نکته قابل توجه آن است که یک شیئ ممکن است در چند دامنه خود را ثبت نماید و لذا دامنه‌ها، برهم‌پوشانی داشته باشند و این موضوع ممکن است منجر به بروز تداخل قواعد حاکم بر اشیاء مشترک گردد که باید به گونه‌ای مرتفع گردد.

در ادامه این بخش پس از معرفی مختصر منطق هنجارها،

[7] Subsumption
[8] Stratified Logic
[9] Temporal Logic
[10] Epistemic Logic
[11] Non-Monotonic

www.SID.ir

مولفه‌های اصلی مدل امنیتی حاکم بر معماری توصیف شده در بالا، تعریف و مورد بررسی قرار می‌گیرند.

۳-۱- منطق هنجارها

منطق هنجارها که به منطق «بایدها و نبایدها» و همچنین منطق «تکلیف» در میان فلاسفه معروف است، برای اولین بار توسط مالِی [۱۵] درسال ۱۹۲۶ به طور صوری بیان گردید و در دهه ۱۹۵۰ توسط وُن‌رایت [۱۶] به طور گسترده‌ای توسعه یافت و متحول گردید. این منطق در واقع توسعه‌ای بر منطق موجهات مشتمل بر عملگرهایی همچون اختیار[12]، الزام[13]، معافیت[14]، حرام[15] و امثالهم می‌باشد و شاخه‌ای از منطق نمادین[16] محسوب می‌گردد [۱۷].

منطق هنجارهای مدنظر در این مقاله حاوی ۴ نوع حکم هنجاری زیر می‌باشد:

- واجب یا لازم است که (OB)
- مجاز است که (PE)
- غیرمجاز یا حرام است که (IM)
- بلامانع است که (GR)

با انتخاب هر یک از چهار حکم اول به عنوان حکم پایه، بقیه احکام را می‌توان بر اساس آن توصیف نمود. به طور معمول حکم واجب (OB) را به عنوان حکم پایه انتخاب می‌نمایند و بقیه را به صورت زیر بر اساس آن بیان می‌نمایند.

$$\mathrm{PE}\ p \leftrightarrow \neg \mathrm{OB} \neg p \qquad \mathrm{IM}\ p \leftrightarrow \mathrm{OB} \neg p \qquad \mathrm{GR}\ p \leftrightarrow \neg \mathrm{OB}\ p$$

با فرض وجود منطق کلاسیک گزاره‌ها، مجموعه‌ای نامحدود از متغیرهای گزاره‌ای، عملگرهای $\rightarrow$ و $\neg$ و عملگر OB، اصول موضوعه A1 تا A3 و قواعد استنتاج R1 و R2 را که در بخش ۲-٤ آمده است می‌توان برای این منطق برشمرد.

۳-۲- مولفه‌های اصلی مدل

ساختار کل مدل به صورت زیر تعریف می‌گردد.

تعریف۱ (ساختار داده مدل امنیتی هنجار مبنا) ساختار داده مدل یک ٤تایی به صورت *(FDS, SPB, MSP, OPR)* می‌باشد، که هر مولفه آن به صورت زیر تعریف می‌شود:

- *FDS*: ساختار داده‌ای مبنا که یک ٦ تایی به صورت *(ONT, CON, SUB, DS, CTX, AU)* می‌باشد که در آن *ONT* شامل آنتالوژی عامل‌ها (O_S)، اشیاء (O_O) و اَعمال (O_A) می‌باشد. $CON=S \cup O \cup A$ مجموعه تمام مفاهیم موجود در این آنتالوژی‌ها و *SUB* مجموعه همه روابط شمول قابل استنتاج بین مفاهیم موجود در آنتالوژی‌ها است. نحوه استخراج *SUB* از آنتالوژی‌ها در مقالات قبلی ما از جمله [۵] آمده است.. $DS=\{OB, PE, IM, GR\}$ انواع احکام قابل وضع در خصوص انجام اَعمال بر اشیاء را درخود دارد. *CTX* یک مجموعه محدود از گزاره‌های توصیف‌کننده زمینه است. $AU=\{u_0,\ldots,u_n\}$ نیز یک مجموعه محدود از مدیران امنیتی (مجازشمارها) را در خود دارا می‌باشد.
- *SPB*: پایگاه قواعد امنیتی یا قواعد دسترسی صریح که جزئیات بیشتر در خصوص قواعد امنیتی و ساختار نحوی آن، به بخش‌های بعد موکول می‌گردد.
- *MSP*: مجموعه فراخط‌مشی‌های سیستم شامل خط‌مشی پیش‌فرض در دسترسی به منابع و خط‌مشی رفع تداخل.
- *OPR*: مجموعه‌ای شامل اَعمال مدیریتی از جمله اضافه و یا حذف نمودن یک قاعده امنیتی و رویه تصمیم‌گیری در خصوص تقاضاهای دسترسی.

با توجه به مدل داده‌ای ارائه شده، مجموع *SPB*، *SUB*، *CTX*، و قواعد رفع تداخل *(RR)* پایگاه دانش این مدل را تشکیل می‌دهد که آن را با *KB* نمایش می‌دهیم. بر این اساس هر گونه استنتاج در این مدل بر پایه مفروضات موجود در *KB* انجام می‌پذیرد. $KB = SPB \cup SUB \cup CTX \cup RR$

۴- توصیف منطقی خط‌مشی‌های امنیتی

بخش اصلی هر مدل امنیتی نحوه توصیف خط‌مشی‌های امنیتی و استنتاج قواعد امنیتی ضمنی از قواعد صریح توصیف شده توسط مدیران امنیتی می‌باشد که در ادامه ساختار نحوی زبان

[12] Permission
[13] Obligation
[14] Prohibition
[15] Impermissible
[16] Symbolic logic

www.SID.ir

مبتنی بر منطق برای توصیف خط‌مشی‌ها به همراه اصول موضوعه، قواعد استنتاج و معناشناسی آن ارائه می‌گردد.

۴-۱- ساختار نحوی

الفبای زبان توصیف خط‌مشی امنیتی در این مدل همان عناصر موجود در مولفه FDS ساختار داده‌ای ارائه شده برای مدل به انضمام رابطهای منطقی $\wedge$ و $\neg$ (یا رابطهای دیگری چون $\vee$ و $\rightarrow$)، یک مسند سه‌تایی $do(s,o,a)$ می‌باشد که در آن $s \in S, o \in O, a \in A$ می‌باشد.

تعریف۲ (فرمول) یک فرمول به صورت بازگشتی بدین شکل تعریف می‌شود؛ هر گزاره زمینه ($x_i \in CTX$) یک (اتمی) است، هر رابطه شمول بین مفاهیم ($C_i \sqsubseteq C_j$) یک فرمول (اتمی) است، هر رابطه سه‌تایی $do(s,o,a)$ که در آن $s \in S, o \in O, a \in A$ یک فرمول (اتمی) است، اگر a و b دو فرمول باشند، $a \wedge b$ و $\neg a$ (و همچنین $a \vee b$ و $a \rightarrow b$) نیز هر کدام یک فرمول هستند، اگر ds یک حکم ($\mathrm{ds} \in DS$) باشد، و u یک مدیر امنیتی ($u \in AU$) و a یک فرمول اتمی باشد، آنگاه $\mathrm{ds}_u\ a$ نیز یک فرمول است.

تعریف ۳ (قاعده امنیتی) هر قاعده امنیتی اعلان شده توسط یک مدیر امنیتی یک فرمول به صورت $\alpha \rightarrow \mathrm{ds}_u\, do(s,o,a)$ می‌باشد که در آن α یک فرمول و $s \in S, o \in O, a \in A, u \in AU, \mathrm{ds} \in DS$ است.

لازم به ذکر است که مجموعه قواعد امنیتی تعریف شده با استفاده از زبان بالا در SPB ذخیره می‌شوند.

۴-۲ نظریه برهان

نظریه برهان در هر منطق شامل دو بخش اصلی مجموعه اصول موضوعه و مجموعه قواعد استنتاج می‌باشد که در واقع دستگاه استنتاجی منطق را بر مبنای ساختار نحوی ارائه شده برای آن شکل می‌دهد. اصول موضوعه و قواعد استنتاج منطق ارائه شده در این مقاله به صورت زیر تعریف می‌گردد.

A1. If p is a tautology of propositional logic, then $\vdash p$ (TAUT)

A2. $\vdash \mathrm{OB}_u(p \rightarrow q) \rightarrow (\mathrm{OB}_u p \rightarrow \mathrm{OB}_u q)$ (OB-K)

A3. $\vdash \mathrm{OB}_u p \rightarrow \neg \mathrm{OB}_u \neg p$ (OB-D)

R1. If $\vdash p$ and $\vdash p \rightarrow q$ then $\vdash q$ (MP)

R2. If $\vdash p$ then $\vdash \mathrm{OB}_u p$ (OB-ONCE)

R3. If $\vdash C \sqsubseteq C'$ then (SI)
$\vdash p(D_1,\ldots,D_i,C',D_{i+1},\ldots,D_n) \rightarrow p(D_1,\ldots,D_i,C,D_{i+1},\ldots,D_n)$

همانطور که قبلاً بیان شد، رابطه کلیدی در تکنولوژی معنایی، رابطه شمول است. این رابطه موجب ایجاد یک سلسله‌مراتب از مفاهیم موجود در هر یک از حوزه‌های عامل‌ها، اشیاء و اَعمال می‌گردد. مهم‌ترین مساله در تامین امنیت و کنترل دسترسی در محیط‌های اگاه از معنا، بررسی تاثیر این رابطه بر انتشار قواعد امنیتی می‌باشد. در مجموعه قواعد استنتاج فوق نیز قاعده SI در واقع تاثیر رابطه شمول را بر منطق ارائه شده برای کنترل دسترسی موجب می‌گردد. بر این اساس می‌توان قضیه زیر را در خصوص انتشار قواعد امنیتی بر مبنای این منطق مطرح نمود.

قضیه۱ (انتشار قواعد امنیتی) اگر دوعامل s و s' وجود داشته باشند که رابطه $s \sqsubseteq s'$ بین آنها برقرار باشد، آنگاه قواعد انتشار زیر قابل استنتاج است

$$\vdash \mathrm{OB}_u do(s',o,a) \rightarrow \mathrm{OB}_u do(s,o,a)$$
$$\vdash \mathrm{PE}_u do(s',o,a) \rightarrow \mathrm{PE}_u do(s,o,a)$$
$$\vdash \mathrm{IM}_u do(s,o,a) \rightarrow \mathrm{IM}_u do(s',o,a)$$

قواعدی مشابه قواعد فوق، در حوزه اشیاء و اَعمال نیز متصور است.

اثبات: به سادگی با اِعمال قاعده استنتاج SI، اصول موضوعه OB-K و MP و رابطه همیشه درست $p \rightarrow q \equiv \neg q \rightarrow \neg p$ (در منطق‌های یکنوا) روابط فوق قابل اثبات است.□

۴-۳- معناشناسی

رایج‌ترین ابزار ارائه معناشناسی برای زبانهای خانواده منطق موجهات، ساختار کریپکی[۱۷] می‌باشد. در این ساختار، مجموعه‌ای از دنیاها (W)، رابطه بین دنیاها (R)، و یک تابع تفسیر (از عناصر اتمی موجود در زبان به مجموعه‌ای از دنیاها)، مولفه‌های اصلی ارائه معناشناسی در منطق مورد نظر می‌باشد.

[17] Kripke Structure

www.SID.ir

Archive of SID

برای تعریف معناشناسی مدل امنیتی مبتنی بر منطق ارائه شده در این مقاله نیز از یک ساختار ۵ تایی $M=\langle W,R,\phi,\Delta,I\rangle$ استفاده می‌نماییم که عناصر آن به صورت زیر تعریف می‌شوند:

- W یک مجموعه غیرتهی از دنیاهای ممکن می‌باشد. هر دنیا در واقع یک حالت سراسری از وضعیت امنیتی محیط آگاه از معنای تحت حفاظت ما می‌باشد.
- $R=AU\to P(W\times W)$ یک تابع تفسیر است که به هر مدیر امنیتی یک رابطه دودویی بر روی دنیاها اختصاص می‌دهد. باید توجه داشت که هر رابطه $R(u)$ یک رابطه سریال است؛ بدین معنی که به ازای هر $w\in W$ وجود دارد حداقل یک $w'\in W$ که $R(u)(w)=w'$.
- $\phi=AtomicFormulas\to P(W)$ یک تابع تفسیر که به هر فرمول اتمی، مجموعه دنیاهایی که در آنها فرمول مورد نظر صادق می‌باشد را نسبت می‌دهد.
- Δ یک مجموعه غیرتهی از اشیاء موجود در تمام دنیاهای W را مشخص می‌نماید. در محیط‌های آگاه ازمعنا این فرض را داریم که تمام دنیاها، یک دامنه شیئ مشترک دارند.
- I یک تابع تفسیر است که در هر دنیا مثل w به هر مفهوم C، یک مجموعه $C_w^I\subseteq\Delta$، به هر مسند بر روی مفاهیم موجود در W مانند $P(C_1,\ldots,C_k)$ یک رابطه kتایی $P_w^I\subseteq\Delta^k$ که یک مجموعه از تاپل‌های kتایی $\langle C_{1w}^I,\ldots,C_{kw}^I\rangle$ است، نسبت می‌دهد و به هر نمونه[18] یک شیئ $d_w^I\in\Delta$ نسبت می‌دهد. تابع تفسیر I، بر اساس تعریف آنتالوژی باید این محدودیت را ارضاء نماید که تفسیر یکسانی را برای مفاهیم و نمونه‌ها در دنیاهای مختلف ارائه نماید. به عبارتی دیگر

$$\text{for all } w,w'\in W:\quad I(w)(C)=I(w')(C)\wedge I(w)(d)=I(w')(d)$$

تفسیر دو مفهوم خاص همگانی (T) و تهی ($\bot$) به صورت زیر می‌باشد.

$$\text{for all } w\in W: I(w)(\mathsf{T})=\mathsf{T}_w^I=\Delta$$
$$\text{for all } w\in W: I(w)(\bot)=\bot_w^I=\varnothing$$

تابع ϕ نیز باید این شرط را ارضاء نماید که برای هر مسند p، $w\in\phi(p)$ اگر و تنها اگر یک مجموعه از تاپل‌های kتایی در دنیای w وجود داشته باشد که تابع I به مسند p منتسب نماید.

تابع ϕ را می‌توان به تابع Φتوسعه داد تا بتوان فرمول‌های پیچیده را نیز تفسیر نمود. تعریف بازگشتی Φدر زیر آمده است.

$$\Phi(p)=\phi(p),\ \text{if } p \text{ is an atomic formula}$$
$$\Phi(\neg\alpha)=W-\Phi(\alpha)$$
$$\Phi(\alpha\wedge\alpha')=\Phi(\alpha)\cap\Phi(\alpha')$$
$$\Phi(C\sqsubseteq C')=\begin{cases}W & \text{,if for all } w\in W:\\ & \quad I(w)(C)\subseteq I(w)(C'),C_w^I\subseteq C_w'^I\\ \varnothing & \text{,otherwise}\end{cases}$$
$$\Phi(\mathrm{OB}_u\alpha)=\{w\,|\,R(u)(w)\subseteq\Phi(\alpha)\}$$
$$\Phi(\mathrm{IM}_u\alpha)=\{w\,|\,R(u)(w)\subseteq\Phi(\neg\alpha)\}$$
$$\Phi(\mathrm{PE}_u\alpha)=\{w\,|\,R(u)(w)\cap\Phi(\alpha)\neq\varnothing\}$$
$$\Phi(\mathrm{GR}_u\alpha)=\{w\,|\,R(u)(w)\cap\Phi(\neg\alpha)\neq\varnothing\}$$

لم۱ (درستی[19] قاعده استنتاج SI): قاعده استنتاج SI، بر مبنای معناشناسی ارائه شده یک قاعده درست می‌باشد.

اثبات: اگر $C\sqsubseteq C'$ باشد، آنگاه برای همه $w\in W$ داریم: $I(w)(C)\subseteq I(w)(C')$ و به عبارت دیگر برای هر $c\in C_w^I$ داریم: $c\in C_w'^I$.

با داشتن مسند $P(D_1,\ldots,D_i,C',D_{i+1},\ldots,D_k)$، در هر دنیای w متعلق به مجموعه دنیاهای $\Phi(P(D_1,\ldots,D_i,C',D_{i+1},\ldots,D_k))$ مسند $P(D_1,\ldots,D_i,C',D_{i+1},\ldots,D_k)$درست است، به عبارت دیگر $\models_w^I P(D_1,\ldots,D_i,C',D_{i+1},\ldots,D_k)$ و درنتیجه طبق معناشناسی، یک مجموعه از تاپل‌های kتایی وجود دارند به قسمی که:

$$P_w'^I=\{\langle d_1,\ldots,d_i,c,d_{i+1},\ldots,d_k\rangle\,|\,c\in C_w'^I,d_j\in D_{jw}^I(1\le j\le k)\}$$

از آنجا که برای هر $c\in C_w^I$ داریم $c\in C_w'^I$، لذا یک مجموعه

$$P_w^I=\{\langle d_1,\ldots,d_i,c,d_{i+1},\ldots,d_k\rangle\,|\,c\in C_w'^I,d_j\in D_{jw}^I(1\le j\le k)\}$$

داریم که $P_w^I\subseteq P_w'^I$. پس می‌توانیم این نتیجه را بگیریم که مسند $P(D_1,\ldots,D_i,C',D_{i+1},\ldots,D_k)$ نیز در دنیای w درست است و به عبارت دیگر $\models_w^I P(D_1,\ldots,D_i,C,D_{i+1},\ldots,D_k)$.

بنابراین براساس تفسیر رابطه $\to$، نتیجه می‌گیریم

$$\models_w^I P(D_1,\ldots,D_i,C',D_{i+1},\ldots,D_k)\to P(D_1,\ldots,D_i,C,D_{i+1},\ldots,D_k)$$

و در نتیجه قاعده استنتاج SI، یک قاعده درست است.□

قضیه۲ (درستی منطق): منطق ارائه شده، یک منطق درست است، یعنی اگر $\vdash A$ آنگاه $\models A$.

[18] Individual

[19] Soundness

www.SID.ir

Archive of SID

اثبات: با توجه به درستی اصول موضوعه A1 تا A3 و قواعد استنتاج R1 و R2 در منطق هنجارها [۱۷] و درستی قاعده استنتاج R3 (قاعده SI) بر اساس لم ۱، می‌توان نتیجه گرفت که منطق و دستگاه استنتاج ارائه شده، نیز درست است.

قضیه۳ (کامل بودن منطق): منطق ارائه شده، کامل است، یعنی اگر $\models A$ آنگاه $\vdash A$.

اثبات: اثبات کامل بودن این منطق در این مقاله نمی‌گنجد. □

۵- مدیریت مدل

مدیریت مدل را از دو بُعد، فراخط‌مشی‌های مدل و اَعمال مدیریتی تعریف شده برای مدل می‌توان بررسی کرد. فراخط‌مشی، درواقع قواعد حاکم بر خط‌مشی‌ها و قواعد امنیتی را بیان می‌نماید و اَعمال مدیریتی نیز، مجموعه اَعمالی که برای تعریف و یا تغییر قواعد امنیتی و اِعمال آن در هر دامنه امنیتی توسط یک مدیر امنیتی مورد نیاز است را مشخص می‌نماید.

۵-۱- فراخط‌مشی مدل

فراخط‌مشی در این مدل شامل دو مولفه اصلی است؛ $MSP=(DefSt, ResSt)$. مولفه اول یعنی $DefSt$ سیاست پیش‌فرض را در خصوص دسترسی‌هایی که هیچ قاعده امنیتی در مورد آن قابل استنتاج نمی‌باشد، مشخص می‌نماید. بر این اساس $DefSt$ می‌تواند یکی از اَحکام {PE, IM, GR} را درخود دارا باشد. مولفه دوم یعنی $ResSt$ نیز استراتژی رفع تداخل را مشخص می‌نماید و می‌تواند یکی از مقادیر $\{NO, PO\}$ را در خود دارا باشد.

تعریف۴ (اَحکام متداخل): دو حکم $\mathrm{ds}_i\,\alpha$ و $\mathrm{ds}_j\,\alpha$ از مجموعه اَحکام DS را متداخل گویند، اگر ریشه در یک از دو زوج متداخل (OB α, OB $\neg\alpha$) و یا (OB α, $\neg$OB α) داشته باشند.

تعریف ۵ (مجموعه متداخل از قواعد امنیتی): یک مجموعه از قواعد امنیتی صریح و یا استنتاج شده $\{p_1,\ldots,p_n\}$، که در آن $p_i = \alpha_i \rightarrow \mathrm{ds}_{i_{u_j}} do(s_i,o_i,a_i)$ می‌باشد، یک مجموعه متداخل از قواعد امنیتی را در یک لحظه خاص تشکیل می‌دهند، اگر

۱. $\alpha_n,\ldots,\alpha_1$ هم‌زمان در آن لحظه ارضاء شده باشند،

۲. عامل‌ها، اشیاء و اعمال قواعد در تداخل با هم باشند:

$$(s_1 \sqcap \cdots \sqcap s_n)^{\mathcal{I}} \neq \emptyset \wedge$$
$$(o_1 \sqcap \cdots \sqcap o_n)^{\mathcal{I}} \neq \emptyset \wedge (a_1 \sqcap \cdots \sqcap a_n)^{\mathcal{I}} \neq \emptyset$$

۳. به ازای هر p_i $(1 \le i \le n)$ وجود داشته باشد یک p_j $(1 \le j \le n)$ که در آنها $\mathrm{ds}_i\,\alpha$ و $\mathrm{ds}_j\,\alpha$ دو حکم متداخل باشند.

دو استراتژی ممکن برای رفع تداخل، استراتژی الویت الزام مثبت بر منفی[20] (PO) و استراتژی الویت الزام منفی بر مثبت[21] (NO) می‌باشد. مجموعه قواعدی که موجب اِعمال هر یک از این دو استراتژی می‌گردد، در جدول ۱ آمده است.

جدول ۱: مجموعه قواعد منطقی لازم برای اِعمال دو استراتژی رفع تداخل

استراتژی	قواعد رفع تداخل (RR)
NO	$\mathrm{OB}_u do(s,o,a) \wedge \neg\mathrm{OB}_v do(s,o,a) \rightarrow \mathrm{OB}_{cr} do(s,o,a)$ $\mathrm{OB}_u \neg do(s,o,a) \wedge \neg\mathrm{OB}_v \neg do(s,o,a) \rightarrow \neg\mathrm{OB}_{cr} \neg do(s,o,a)$ $\mathrm{OB}_u do(s,o,a) \wedge \mathrm{OB}_v \neg do(s,o,a) \rightarrow \mathrm{OB}_{cr} do(s,o,a)$
PO	$\mathrm{OB}_u do(s,o,a) \wedge \neg\mathrm{OB}_v do(s,o,a) \rightarrow \neg\mathrm{OB}_{cr} do(s,o,a)$ $\mathrm{OB}_u \neg do(s,o,a) \wedge \neg\mathrm{OB}_v \neg do(s,o,a) \rightarrow \mathrm{OB}_{cr} \neg do(s,o,a)$ $\mathrm{OB}_u do(s,o,a) \wedge \mathrm{OB}_v \neg do(s,o,a) \rightarrow \mathrm{OB}_{cr} \neg do(s,o,a)$

لازم به توضیح است که در این روابط، مدیر امنیتی cr یک مدیر امنیتی خاص است که دامنه آن همه اشیاء می‌باشد و صرفاً برای میانجی‌گری در زمان بروز تداخل بین اَحکام صادره از سوی دو مدیر امنیتی وارد عمل می‌شود.

۵-۲- اعمال مدیریتی

در مجموع سه عمل زیر را هر مدیر امنیتی در حوزه خویش برای تدوین قواعد امنیتی، بروزرسانی آنها و اِعمال آنها نیاز دارند:

AddPolicyRule: برای اضافه نمودن یک قاعده امنیتی توسط یک مدیر امنیتی به پایگاه قواعد امنیتی به شرط آنکه قبل از آن قاعده‌ای نقیض آن را بیان نکرده باشد. به عبارت دیگر پیش‌نیاز اضافه نمودن قاعده $\alpha \rightarrow \mathrm{ds}_u do(s,o,a)$ برقراری شرط زیر

[20] Positive Obligation Take Precedence
[21] Negative Obligation Take Precedence

www.SID.ir

Archive of SID

می‌باشد: $KB \wedge \alpha \rightarrow ds_u do(s,o,a) \not\vdash \sim$ (تناقض)

RemovePolicyRule: برای حذف یک قاعده از پایگاه قواعد امنیتی توسط یک مدیر به کار می‌رود و پیش‌شرط خاصی ندارد.

AccessDecision: برای اِعمال کنترل دسترسی بر اساس قواعد امنیتی وضع شده، در زمان دریافت یک درخواست دسترسی از سوی یک عامل به کار می‌رود. از آنجایی‌که یک شیئ ممکن است تحت حفاظت چند مدیر امنیتی باشد، لازم است که هر مدیر امنیتی در بررسی تقضاهای دسترسی به یک شیئ مشترک، با دریافت نظرات مربوط به مدیران دیگر بر اساس الگوریتم ۱ عمل نماید. این الگوریتم، در واقع ابتدا وجود تداخل را چک می‌کند و در صورت وجود، نظر cr را استنتاج می‌نماید. در صورت عدم استنتاج از cr (یعنی عدم وجود تداخل)، سعی می‌کند تا حکم موجود بر روی شیئ مورد دسترسی را از هر یک از مدیران آن استنتاج نماید، در صورت عدم وجود هیچ گونه حکمی بر روی شیئ موردنظر، حکم پیش‌فرض را برمی‌گرداند. باید این نکته را متذکر شد که این الگوریتم کلی در عمل می‌تواند به شکل کارایی پیاده‌سازی شود که در این نوشتار مجال بیان آن نیست. علاوه‌براین با توجه به برخی محدودیت‌های اِعمال شده در مدل از جمله محدود بودن تعداد مدیران امنیتی سیستم، الگوریتم ارائه شده، تصمیم‌پذیر می‌باشد.

الگوریتم ۱: الگوریتم تصمیم‌گیری در خصوص تقاضاهای دسترسی

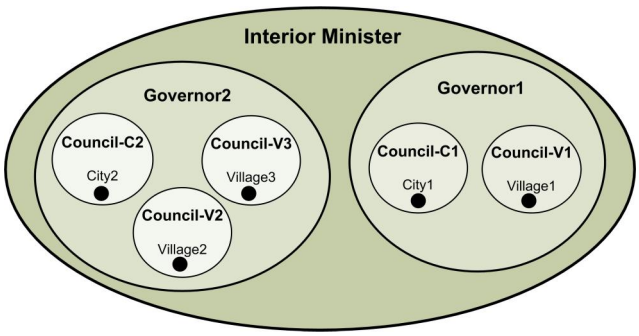
Algorithm 1 AccessDecision($s \in S, o \in O, a \in A$)

1: **if** $KB \vdash \mathtt{PE}_{cr} do(s,o,a)$ **then**
2: **return** Permitted
3: **end if**
4: **if** $\exists u \in AU : KB \vdash \mathtt{PE}_u\ do(s,o,a)$ **then**
5: **return** Grant
6: **end if**
7: **if** $\exists v \in AU : KB \vdash \mathtt{IM}_v\ do(s,o,a)$ **then**
8: **return** Deny
9: **end if**
10: **if** $DefSt = \mathtt{IM}$ **then**
11: **return** Deny
12: **else**
13: **return** Grant
14: **end if**

۶- مطالعه موردی

برای تفهیم بیشتر نحوه توصیف خط‌مشی‌ها و استنتاج آنها بر مبنای مدل منطقی ارائه شده، در این بخش به طور مختصر به ارائه یک نمونه کاربرد این مدل در یک سیستم انتخابات جامع (ES) می‌پردازیم. این سیستم به صورت توزیع‌شده عمل می‌نماید و شامل سیستم انتخابات ریاست جمهوری (PES)، سیستم انتخابات شهردار (MES)، و سیستم انتخابات مجلس (LES) می‌باشد. از هر یک از سه سیستم فوق، یک نمونه از آن در هر شهر یا روستا نصب می‌شود و به ارائه سرویس می‌پردازد. انتخابات در هر شهر یا روستا به وسیله شورای انتخابات (Council) شهر یا روستا مدیریت و کنترل می‌شود و سیستم‌های انتخاباتی یک شهر و روستاهای متعلق به آن توسط یک فرماندار (Governor) مدیریت می‌گردد و نهایتاً کل سیستم‌های انتخاباتی زیر نظر وزیر کشور (Interior Minister) هدایت و راهبری می‌گردد. شکل ۱ توصیف آنتالوژی سیستم‌ها (اشیاء) تحت حفاظت را به زبان منطق توصیفی و ساختار مدیریت سیستم‌ها را نشان می‌دهد.

$$\mathrm{ES} = \mathrm{PES} \sqcup \mathrm{MES} \sqcup \mathrm{LES}$$
$$\mathrm{PES} = \mathrm{pes}_{c_1} \sqcup \mathrm{pes}_{c_2} \sqcup \mathrm{pes}_{v_1} \sqcup \mathrm{pes}_{v_2} \sqcup \mathrm{pes}_{v_3}$$
$$\mathrm{MES} = \mathrm{mes}_{c_1} \sqcup \mathrm{mes}_{c_2}$$
$$\mathrm{LES} = \mathrm{les}_{c_1} \sqcup \mathrm{les}_{c_2} \sqcup \mathrm{les}_{v_1} \sqcup \mathrm{les}_{v_2} \sqcup \mathrm{les}_{v_3}$$



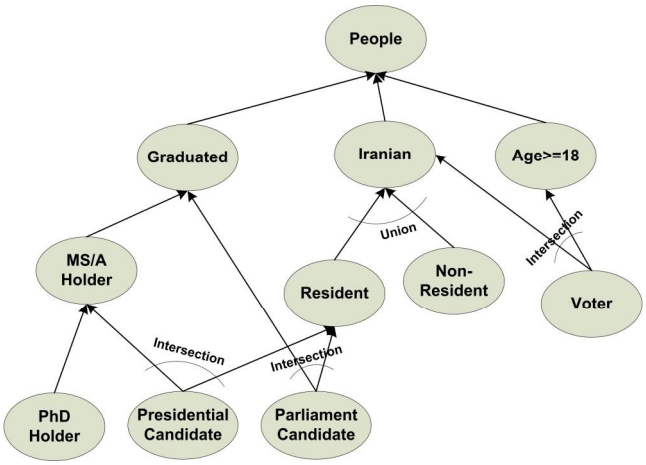
شکل ۱: توصیف سیستم‌های تحت حفاظت و دامنه‌های امنیتی هریک از مدیران امنیتی

توصیف بخشی از آنتالوژی عامل‌های موجود در سیستم به همراه نمایش نمادین آن در شکل ۲ آمده است. وجود پیکان از A به B به معنای آن است که B شامل A می‌باشد.

در این مثال مجموعه اَعمالی (آنتالوژی اَعمالی) که می‌توان بر روی اشیاء (سیستم‌های انتخاباتی) انجام داد به صورت زیر می‌باشد.

$A=\{vote, startCount, register, viewResult\}$

www.SID.ir



$\text{Iranian} \sqsubseteq \text{People}$
$\text{Age} >= 18 \sqsubseteq \text{People}$
$\text{Iranian} \equiv \text{Resident} \sqcup \text{NonResident}$
$\text{Graduated} \sqsubseteq \text{People}$
$\text{MS/A Holder} \sqsubseteq \text{Graduated}$
$\text{PhD Holder} \sqsubseteq \text{MS/A Holder}$
$\text{PresCand} \equiv \text{MS/A Holder} \sqcap \text{Resident}$
$\text{ParlCand} \equiv \text{Graduated} \sqcap \text{Resident}$
$\text{Voter} \equiv \text{Iranian} \sqcap \text{Age} >= 18$

شکل ۲: توصیف آنتالوژی عامل‌ها به همراه نمایش نمادین آن

مجموعه گزاره‌های توصیف‌کننده زمینه نیز به صورت زیر می‌باشد.

$CTX = \{p_0, p_1, p_2, p_3, p_4\}$
p_0 = time is 8am-18pm
p_1 = date is 2007/5/21
p_2 = date is 2007/3/31-2007/3/15
p_3 = time is after 21pm of 2007/3/25
p_5 = time is after 19pm of 2007/5/21

در این شرایط می‌توان قواعد امنیتی زیر را به طور نمونه توصیف نمود:

۱. کسانی که مقیم ایران بوده و حداقل دارای مدرک کارشناسی ارشد باشند در بازه زمانی ۲۰۰۷/۲/۱۵ تا ۲۰۰۷/۳/۳۱ می‌توانند به عنوان کاندیدای ریاست‌جمهوری در هر یک از سیستم‌های انتخابات ریاست‌جمهوری ثبت‌نام نمایند.

$\text{PresCand} \equiv \text{MS/A Holder} \sqcap \text{Resident}$
$p_2 \rightarrow \text{PE}_{\text{InteriorMinister}}\ \boldsymbol{do}(\text{PresCand, PES, register})$

۲. کسانی که مقیم ایران بوده و حداقل دارای مدرک کارشناسی باشند در بازه زمانی ۲۰۰۷/۳/۲۵ تا ۲۰۰۷/٤/۵ می‌توانند به عنوان کاندیدای نمایندگی مجلس در هر یک از سیستم‌های انتخابات مجلس ثبت‌نام نمایند.

$\text{ParlCand} \equiv \text{Graduated} \sqcap \text{Resident}$
$p_4 \rightarrow \text{PE}_{\text{InteriorMinister}}\ do(\text{ParlCand, PES, register})$

۳. کسانی می‌توانند در انتخابات ریاست‌جمهوری و مجلس در روز ۲۰۰۷/۵/۲۱ در بازه ۸ صبح تا ۱۸ عصر رای دهند که حداقل ۱۸ سال داشته و ایرانی باشند.

$\text{Voter} \equiv \text{Iranian} \sqcap \text{Age} >= 18$
$p_0 \wedge p_1 \rightarrow \text{PE}_{\text{InteriorMinister}}\ \boldsymbol{do}(\text{Voter, ES, vote})$

٤. بر اساس حکم فرماندار ۱ (Governor1) شمارش آراء در شهر۱ باید تا حداکثر سه ساعت پس از پایان انتخابات و در روستاهای آن تا حداکثر یک ساعت پس از اتمام انتخابات آغاز گردد.

$\text{ES}_{C_1} \equiv \text{pes}_{c_1} \sqcup \text{les}_{c_1} \sqcup \text{mes}_{c_1}$
$\text{ES}_{V_1} \equiv \text{pes}_{v_1} \sqcup \text{les}_{v_1} \sqcup \text{mes}_{v_1}$
$p_3 \rightarrow \text{OB}_{\text{Governor1}}\ \boldsymbol{do}(\text{CommitteeC1}, \text{ES}_{C_1}, \text{startCount})$
$p_5 \rightarrow \text{OB}_{\text{Governor1}}\ \boldsymbol{do}(\text{CommitteeV1}, \text{ES}_{V_1}, \text{startCount})$

فرض کنید که یک درخواست برای کاندیداتوری مجلس و ریاست جمهوری درتاریخ ۲۰۰۷/۳/۲۰ از سوی فرد x که دارای مدرک کارشناسی و مقیم ایران است، در شهر ۱ دریافت می‌گردد. سیستم پس از وارسی صحت گواهی‌های ارائه شده، دو رابطه زیر به پایگاه دانش خود اضافه می‌نماید.

$$x \sqsubseteq \text{Graduated} \qquad x \sqsubseteq \text{Resident}$$

بر اساس قاعده امنیتی (۱) و روابط شمول، سیستم به صورت منطقی احکام زیر را استنتاج می‌نماید که معنی آن این است که فرد x می‌تواند به عنوان کاندیدای نمایندگی مجلس در شهر ثبت‌نام نماید، اما به عنوان کاندیدای ریاست جمهوری نمی‌تواند ثبت‌نام نماید.

$$\text{IM}_{\text{InteriorMinister}}\ \boldsymbol{do}(x, \text{pes}_{C_1}, \text{rgister})$$
$$\text{PE}_{\text{InteriorMinister}}\ \boldsymbol{do}(x, \text{les}_{C_1}, \text{register})$$

۷- جمع‌بندی و کارهای آتی

در این مقاله یک مدل امنیتی اولیه مبتنی بر ترکیب منطق هنجارها و منطق توصیفی برای توصیف و اِعمال خط‌مشی‌های امنیتی در محیط‌های آگاه ازمعنا ارائه گردید. تبدیل روابط معنایی موجود در محیط در حوزه عامل‌ها، اشیاء و اَعمال به

www.SID.ir

Archive of SID

رابطه شمول و استفاده از منطق در این مدل، این امکان را به آن داده است که انواع کانال‌های استنتاج موجود در محیط، قابل کنترل باشند و تاثیر وضع یک قاعده امنیتی بر اساس روابط معنایی موجود انتشار یابد. علاوه‌براین، مدل ارائه شده یک مدل مبتنی بر گواهی خصوصیت است و محدودیت‌های زمینه‌ای نیز با امکاناتی محدود در آن قابل توصیف می‌باشد.

با وجود مزایای بسیار برای مدل ارائه شده، لازم است که موارد زیر در مرحله بعدی این پژوهش توسعه یابد:

- تبیین ارتباط بین ساختار کریپکی و مفهوم دنیاها در آن با مفهوم فضای حالت امنیتی (حالت حفاظتی[۲۲]).
- بررسی قدرت بیان مدل در توصیف انواع خط‌مشی‌ها.
- ارائه یک معماری جهت پیاده‌سازی یک سیستم امنیتی مبتنی بر مدل ارائه شده و ساخت یک نمونه آزمایشگاهی.
- افزودن مفهوم مدیران مرکب[۲۳] به مدل به منظور برخورداری از امکان توصیف خط‌مشی‌ها توسط مدیران به صورت ترکیبی و همچنین تبیین مفهوم وکالت مدیریت.

یکی از خصوصیات قابل توجه در منطق ارائه شده، یکنوا[۲۴] بودن آن می‌باشد که با توجه به برخی نیازهای امنیتی در محیط‌های آگاه از معنا از جمله نیاز به بیان قواعد استثناء، یک نقطه ضعف عمده به شمار می‌رود. در این راستا پس از تکمیل نسخه یکنوای این منطق، قصد ارائه نسخه غیریکنوای آن را داریم که در مراحل بعدی این پژوهش بدان خواهیم پرداخت.

۸- مراجع

[1] F. Baader, D. Calvanese, D. L. McGuinness, D. Nardi, and P. F. Patel-Schneider, *The Description Logic Handbook: Theory, Implementation, and Applications*. New York, NY, USA: Cambridge University Press, 2003.

[2] P. A. Bonatti, C. Duma, N. Fuchs, W. Nejdl, D. O. and, J. Peer, and N. Shahmehri, "Semantic Web Policies - A Discussion of Requirements and Research Issues," presented at 3rd European Semantic Web Conference (ESWC), Budva, Montenegro, 2006.

[3] L. Kagal, T. Finin, and A. Joshi, "A Policy-Based Approach to Security for the Semantic Web," presented at 2nd International Semantic Web Conference (ISWC'03), Sanibel Island, Florida, USA, 2003.

[4] L. Qin and V. Atluri, "Concept-Level Access Control for the Semantic Web," presented at ACM Workshop on XML Security, Fairfax, VA, USA, 2003.

[5] S. Javanmardi, M. Amini, and R. Jalili, "An Access Control Model for Protecting Semantic Web Resources," presented at 2nd International Semantic Web Policy Workshop (SWPW'06) 2006, Athens, GA, USA, 2006.

[6] J. I .Glasgow, G. H. MacEwen, and P. Panangaden, "Reasoning about Knowledge and Permission in Secure Distributed Systems," presented at First IEEE Computer Security Foundations Workshop (CSFW'88), Franconia, New Hampshire, USA, 1988.

[7] M. Abadi, M. Burrows, B .Lampson, and G. Plotkin, "A Calculus for Access Control in Distributed Systems," *ACM Transactions on Programming Languages and Systems*, vol. 15, pp. 706–734, 1993.

[8] T. Y. C. Woo and S. S. Lam, "Authorization in Distributed Systems: A New Approach," *Journal of Computer Security*, vol. 2, pp. 107-136, 1993.

[9] S. Jajodia, P. Samarati, M. L. Sapino, and V. S. Subrahmanian, "Flexible Support for Multiple Access Control Policies," *ACM Transaction on Database Systems*, vol. 26, pp. 214-260, 2001.

[10] J. B .D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A Generalized Temporal Role-Based Access Control Model," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, pp. 4-23, 2005.

[11] F. Cuppens, "An Epistemic and Deontic Logic for Reasoning about Computer Security," presented at European Symposium on Research in Computer Security, Toulouse, France, 1990.

[12] F. Cuppens, "Roles and Deontic Logic," presented at Second International Workshop on Deontic Logic in Computer Science, Oslo, Norway, 1994.

[13] F. Cuppens and R. Demolombe, "A Deontic Logic for Reasoning about Confidentiality," presented at 3rd International Workshop on Deontic Logic in Computer Science, Sesimbra, Portugal, 1996.

[14] L. Kagal, T. Finin, and A. Joshi, "Trust-based Security in Pervasive Computing Environments," *IEEE Computer*, vol. 34, pp. 154-157, 2001.

[15] E. Mally, "Grundgesetze des Sollens: Elemente der Logik des Willens," Graz: Leuschner und Lubensky, Universitäts-Buchhandlung, viii+85 pp 1926.

[16] G. H. V. Wright, "Deontic Logic," *Mind*, vol. 60, pp. 1-15, 1951.

[17] P. McNamara, "Deontic Logic," in *The Stanford Encyclopedia of Philosophy*, E. N. Zalta, Ed.: Metaphysics Research Lab, CSLI, Stanford University, 2006.

[22] Protection State
[23] Composite Authority
[24] Monotonic

www.SID.ir