Archive of SID

مدلی جدید برای کنترل دسترسی سیستم اسکادا بر اساس استاندارد CIM

پیام محمودی نصر و علی یزدیان ورجانی

چکیده: سیستم‌های اسکادا وظیفه پایش و کنترل زیرساخت‌های حیاتی را به عهده داشته و هر گونه حمله به آنها خسارت‌های جبران‌ناپذیری به همراه دارد. یکی از حملات پرخطر به این سیستم‌ها، حمله خودی است. این حمله زمانی اتفاق می‌افتد که کاربران مجاز با سوء استفاده از مجوزهای قانونی سعی در ایجاد اختلال و از کار انداختن سیستم می‌کنند. از آنجایی که هر گونه سوء استفاده تصادفی و یا عمدی از مجوزها می‌تواند نتایج معکوسی را به همراه داشته باشد، ارائه یک مدل کنترل دسترسی که ضمن اختصاص مجوزهای لازم از فعالیت‌های مخرب و اضافی جلوگیری به عمل آورد ضروری است. این مقاله با بیان نیازمندی‌های کنترل دسترسی سیستم اسکادا، ابتدا مفهوم مدت اعتبار را به مدل کنترل دسترسی اجباری اضافه کرده و سپس با توجه به نوع فعالیت کاربر، وضعیت شبکه، زمان فعال‌شدن نقش‌ها، سطوح امنیتی و مدت اعتبار آنها یک مدل جدید کنترل دسترسی در قالب استاندارد CIM برای سیستم اسکادا در شبکه قدرت ارائه کرده است. به منظور آنالیز مدل پیشنهادی از شبکه‌های پتری رنگی استفاده شده و برای نمایش نحوه پیاده‌سازی مدل، کلاس‌ها و ارتباط‌های مورد نیاز در قالب زبان UML ارائه گردیده است.

***کلیدواژه:* امنیت اسکادا، حملات خودی، کنترل دسترسی، CIM.**

۱- مقدمه

سیستم‌های اسکادا [1](SCADA) در زیرساختارهای حیاتی[2] مختلفی از جمله شبکه‌های توزیع برق، آب، نفت و گاز استفاده شده و امنیت آنها نقش به سزایی در امنیت ملی و فعالیت‌های اقتصادی هر کشوری دارد. این در حالی است که بنا بر گزارش [۱] ۱۸۱ حمله تنها در سال ۲۰۱۳ در رابطه با زیرساخت‌های حیاتی به ثبت رسیده که در بین آنها نقض احراز هویت[3] و سیاست‌های کنترل دسترسی بیشترین سهم، یعنی ۵۸٪ را به خود اختصاص داده است. تاریخچه‌ای از حملات گزارش‌شده به سیستم‌های اسکادا از سال ۱۹۹۹ تا ۲۰۱۳ به همراه اطلاعات تکمیلی آنها در [۲] ارائه شده است.

در سیستم‌های اسکادا اپراتورها نقش اساسی داشته و همواره فرض بر آن است که آنها وظایف خود را به درستی انجام می‌دهند. در حالی که یکی از تهدیدهای خطرناک هنگامی است که کاربران مجاز با سوء استفاده از مجوزهای قانونی و ارسال دستورات مخرب، در شبکه اختلال ایجاد کرده و یک حمله خودی[4] را انجام می‌دهند [۳]. بنا بر گزارش [۴] ۳۳/۳ درصد حملات سیستم‌های اسکادا از سال ۲۰۰۰ تا ۲۰۱۱ از نوع خودی و توسط دیسپاچرها انجام گرفته است. هدف این مقاله ارائه یک مدل کنترل دسترسی در سیستم اسکادا با توجه به نیازمندی‌های آن در شبکه قدرت است.

یکی از بهترین روش‌ها برای مقابله با حملات خودی استفاده از مدل‌های مناسب کنترل دسترسی است [۵]. کنترل دسترسی مدلی برای دسترسی به منابع مشترک در یک سیستم با حفظ محرمانگی[5]، تمامیت[6] و دسترس‌پذیری[7] است [۶]. تا کنون تحقیقات فراوانی در رابطه با مدل‌های کنترل دسترسی و نحوه پیاده‌سازی آن در کاربردهای مختلف و از جمله سیستم اسکادا انجام شده است. مدل استاندارد RBAC[8] در استاندارد IEC -۶۲۳۵۱ -۸ [۷] به عنوان مدل مناسب کنترل دسترسی در شبکه هوشمند الکتریکی[9] معرفی شده است که با استفاده از این مدل تنها کاربران مجاز می‌توانند به تجهیزات شبکه و داده‌های جمع‌آوری شده از آن دسترسی پیدا کنند. در [۱] یک سیستم خبره مبتنی بر نقش به منظور پیاده‌سازی سیاست‌های کنترل دسترسی با توجه به استاندارد IEC -۶۲۳۵۱ -۸ در سیستم‌های قدرت پیشنهاد شده است. در [۸] یک سیستم کنترل دسترسی نقش‌محور و مبتنی بر حوزه مسئولیت کاربر در شبکه الکتریکی هوشمند ارائه شده است. در این مدل نقش‌ها و حوزه‌های مسئولیتی به کاربران اختصاص پیدا کرده و سیاست‌های کنترل دسترسی بر اساس نقش‌ها و حوزه‌های مسئولیتی تنظیم می‌گردند. آن گاه درخواست دسترسی کاربر به شرطی پذیرفته می‌شود که سیاست‌های دسترسی در هر دو بخش آن را مجاز بشمارند. در [۹] یک مدل کنترل دسترسی نقش‌محور مبتنی بر زبان نشانه‌گذاری توسعه‌پذیر (XML)[10] برای سیستم‌های قدرت ارائه شده است. در این مدل ابتدا برای هر کاربر یک مقدار اعتماد[11] محاسبه می‌گردد و سپس نقش‌ها با توجه به مقدار اعتماد به کاربران اختصاص پیدا می‌کند. در [۱۰] نیز از مدل RBAC برای پیاده‌سازی کنترل دسترسی در سیستم اسکادا استفاده شده است. در این مرجع از ابزار UML[12] برای آنالیز و نمایش نیازمندی‌های کنترل دسترسی و از شبکه‌های پتری رنگی (CPN)[13] به منظور آنالیز سیاست‌های کنترل دسترسی استفاده شده است. اگرچه مجموعه این تحقیقات دارای ارزش

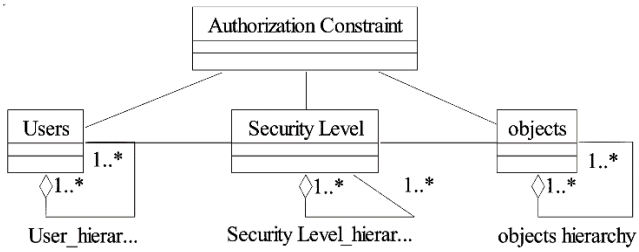
این مقاله در تاریخ ۲۱ اسفند ماه ۱۳۹۳ دریافت و در تاریخ ۲۸ دی ماه ۱۳۹۴ بازنگری شد.

پیام محمودی نصر، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، (email: payam.mahmoudi@modares.ac.ir).
علی یزدیان ورجانی، دانشکده مهندسی برق و کامپیوتر، دانشگاه تربیت مدرس، تهران، (email: yazdian@modares.ac.ir).

1. Supervisory Control and Data Acquisition
2. Critical Infrastructure
3. Authentication
4. Insider Attack
5. Confidentiality
6. Integrity
7. Availability
8. Role Based Access Control
9. Smart Grid
10. Extensible Markup Language
11. Trust
12. Unified Modeling Language
13. Colored Petri Net

www.SID.ir

Archive of SID



شکل ۱: نمودار کلاسی مدل اجباری [۱۱].

فراوانی است اما هر یک از آنها تنها بخشی از نیازمندی‌های کنترل دسترسی را در سیستم پیچیده اسکادا پوشش می‌دهند. این در حالی است که در سیستم‌های پیچیده به دلیل فراوانی نیازمندی‌ها، معمولاً از مدل‌های ترکیبی برای پوشش کامل کنترل دسترسی استفاده می‌شود [۱۱]. در این سیستم‌ها انتخاب مدل‌های مناسب کنترل دسترسی از میان مدل‌های مختلف موجود از نکات مهم برای پیاده‌سازی کنترل دسترسی است. لازمه این انتخاب داشتن شناخت کامل از ساختار اطلاعاتی، تنوع کاربران، گستردگی منابع و فعالیت‌های سیستم است. بر این اساس نوآوری‌های ارائه‌شده در این مقاله عبارتند از:

- افزودن مدت اعتبار سطوح امنیتی به مدل کنترل دسترسی اجباری.
- استفاده از استاندارد CIM[1] ۶۱۹۷۰ -۳۰۱ IEC [۱۲] در طراحی مدل کنترل دسترسی.
- ارائه یک مدل ترکیبی جدید از TBAC[2]، PBAC[3] و DMAC[4] برای کنترل دسترسی سیستم اسکادا در سیستم‌های قدرت.

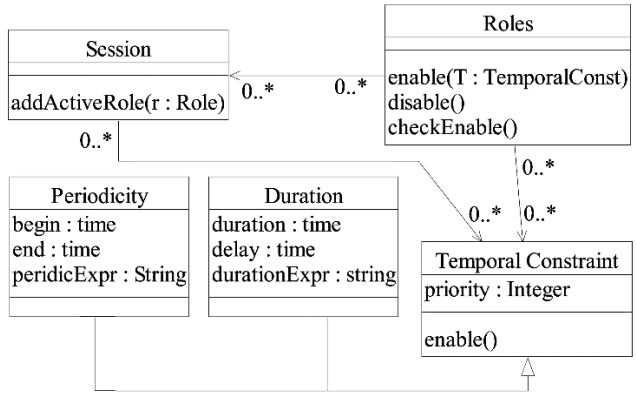
این مقاله با بررسی دقیق نیازمندی‌های کنترل دسترسی در سیستم اسکادا ابتدا به دلیل پویایی سطوح امنیتی داده‌های اسکادا، مفهوم مدت اعتبار را به هسته مدل اجباری اضافه کرده (که در این مقاله با عنوان DMAC شناخته می‌شود) و سپس مدل ترکیبی جدیدی از DMAC، PBAC و TBAC در قالب استاندارد CIM برای کنترل دسترسی سیستم اسکادا در شبکه قدرت ارائه می‌دهد. در این مقاله یک بسته جدید کنترل دسترسی که حاوی کلاس‌های مدل ترکیبی پیشنهادی است برای اضافه‌شدن به مدل استاندارد CIM پیشنهاد شده است.

در ادامه در بخش دوم اطلاعات پیش‌زمینه آورده شده است. بخش سوم مدل ترکیبی پیشنهادی را به همراه کلاس‌های مورد نیاز بر اساس استاندارد CIM و در قالب زبان UML ارائه می‌دهد. بخش چهارم به آنالیز مدل پیشنهادی می‌پردازد و در بخش پنجم نتایج آورده شده است.

۲- پیش‌زمینه

۲-۱ مدل استاندارد CIM

استاندارد CIM توسط سازمان EPRI تهیه شده و هم‌اکنون به عنوان بخشی از استاندارد IEC-۶۱۹۷۰-۳۰x معرفی شده است. استاندارد CIM یک مدل داده‌ای شیءگرا را با هدف یکپارچه‌سازی سیستم‌های نرم‌افزاری در مهندسی قدرت و در قالب زبان UML ارائه کرده است [۱۲]. این استاندارد یک مدل یکپارچه را با هدف به اشتراک‌گذاری داده‌ها میان انواع برنامه‌های کاربردی شبکه قدرت ارائه کرده است. در این استاندارد اگرچه از بسته‌های مختلفی برای جداسازی داده‌ها استفاده گردیده اما پیشنهادی



شکل ۲: نمودار کلاسی مدل TBAC مبتنی بر نقش موقتی [۱۳].

در جهت کنترل دسترسی به داده‌ها ارائه نشده است. بسته‌های مختلف این استاندارد این امکان را فراهم می‌سازند که انواع نرم‌افزارهای مدیریت انرژی به راحتی بتوانند با یکدیگر در ارتباط باشند. این استاندارد از تعدادی بسته و هر بسته از تعداد زیادی کلاس تشکیل شده که عناوین بسته‌ها به شرح زیر است:

Core, Topology, Wires, Outage, Protection, SCADA, Domain, Measurement, LoadModel, Generation.

۲-۲ کنترل دسترسی

کنترل دسترسی مدل مدیریت سطح دسترسی کاربران قانونی به منابع مشترک در یک سیستم است [۶]. هدف از کنترل دسترسی محدودنمودن فعالیت‌هایی است که کاربر قانونی مستقیماً و یا از طریق برنامه‌ها در سیستم انجام می‌دهد.

۲-۲-۱ مدل استاندارد RBAC

مدل استاندارد کنترل دسترسی، مدل نقش مبنا یا RBAC است. در این مدل مجوز دسترسی کاربران به اشیا (منابع) بر اساس نقش آنها تعیین می‌شود. نقش، یک وظیفه شغلی در سازمان است که مسئولیتی را به عهده دارد و به عبارت دیگر هر نقش مجموعه‌ای از مجوزها است. یک کاربر می‌تواند عضو مجموعه‌ای از نقش‌ها باشد. در این مدل نقش‌ها، سلسله‌مراتب نقش‌ها، زمان فعال‌شدن نقش‌ها و محدودیت‌های عضویت کاربران در نقش‌ها از اهمیت به سزایی برخوردار است.

۲-۲-۲ مدل اجباری یا MAC

در مدل کنترل دسترسی به روش اجباری منابع از نظر میزان محرمانگی و کاربران از نظر میزان دسترسی به آنها طبقه‌بندی می‌گردند. کاربر بالاتر مجوز خواندن/نوشتن اطلاعات کاربر پایین‌تر از خود را داشته و کاربر پایین‌تر فقط مجوز نوشتن برای کاربر بالاتر از خود را دارد. کاربرد فراوان مدل اجباری در سازمان‌های نظامی است. در این مدل کاربران و منابع هر کدام به صورت سلسله‌مراتبی طبقه‌بندی می‌شوند. شکل ۱ نمودار کلاسی مدل MAC را نشان می‌دهد [۱۱].

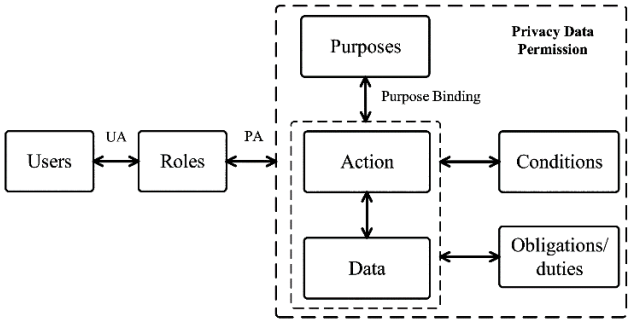
۲-۲-۳ مدل TBAC مبتنی بر نقش موقتی

در مدل TBAC مفهوم زمان فعال‌شدن نقش‌ها به مدل استاندارد RBAC اضافه شده است. در این مدل از دو نوع محدودیت زمانی ۱) محدودیت زمانی با الگو و ۲) محدودیت زمانی برای موارد خاص، هنگام فعال یا غیر فعال شدن نقش‌ها در نشست جاری پشتیبانی می‌شود. شکل ۲ نمودار کلاسی مدل TBAC را نشان می‌دهد [۱۳]. کلاس‌های Duration و Periodicity به ترتیب نحوه پیاده‌سازی وابستگی به

1. Common Information Model
2. Temporal RBAC
3. Privacy RBAC
4. Duration Mandatory Access Control

www.SID.ir

Archive of SID



شکل ۳: مدل PBAC مبتنی بر نقش با حفظ حریم خصوصی [۱۴].

یک زمان خاص و یا یک دوره زمانی با الگو را با توجه به کلاس Temporal Constraint نشان می‌دهند.

۲-۲-۴ مدل PBAC مبتنی بر نقش با حفظ حریم خصوصی

PBAC نوعی مدل کنترل دسترسی مبتنی بر نقش است که در آن ملاحظاتی در خصوص حفظ حریم خصوصی انجام شده است. این ملاحظات عبارتند از ۱) نوع خواسته کاربر، ۲) شرایط دسترسی و ۳) وظایف قابل انجام قبل از دسترسی به اطلاعات. در مواردی که سطح دسترسی به اطلاعات با توجه به شرایط سیستم و نوع خواسته کاربر قابل تغییر است استفاده از مدل PBAC پیشنهاد می‌شود.

شکل ۳ نمودار بلوکی مدل PBAC را نشان می‌دهد [۱۴]. در مدل PBAC بخش‌های کاربر، نقش، داده (منابع سیستم) و عملیات مطابق با مدل RBAC استاندارد است. انواع خواسته کاربر در بخش Purpose و انواع پیش‌شرط‌ها در بخش Condition تعریف می‌شوند. هر گونه مجوز دسترسی به داده‌ها با توجه به نوع خواسته کاربر و شرایط سیستم صادر می‌شود. در بخش Duties مجموعه عملیاتی تعریف می‌گردد که قبل از دسترسی کاربر به داده، لازم به اجرا است.

۲-۳ سیستم اسکادا

سیستم‌های اسکادا وظیفه پایش و کنترل عملیات شبکه‌های صنعتی را به عهده دارند. در این سیستم‌ها داده‌های اندازه‌گیری شده در پست‌ها به وسیله RTU[1] جمع‌آوری و از طریق یک شبکه مخابراتی خصوصی و یا عمومی برای مرکز کنترل ارسال می‌شوند. سرویس‌دهنده HMI[2] در مرکز کنترل داده‌های دریافتی را به اپراتور نمایش داده و بر عکس فرمان‌های کنترلی اپراتور را برای تجهیزات داخل پست‌ها ارسال می‌کند [۱۵]. هر گونه تغییر در شرایط سیستم که نیازمند توجه اپراتور باشد در قالب یک هشدار اعلام خواهد شد. تمامی داده‌ها و فرمان‌ها در سرویس‌دهنده بایگانی[3] ذخیره می‌گردند. این داده‌ها در ارزیابی نحوه عملکرد تجهیزات، بررسی مهارت اپراتور و در تصمیم‌گیری‌های آتی کاربرد فراوان دارد.

نکته دیگر حملات اسکادا است که آنها را می‌توان به دو گروه حملات خودی (داخلی) و غیر خودی (خارجی) تقسیم کرد. حملات غیر خودی توسط کاربران غیر مجاز و خارج از سیستم مانند هکرها و دولت‌های متخاصم انجام شده در حالی که حملات خودی توسط کاربران مجاز و با سوء استفاده از مجوزهای قانونی انجام می‌شود. اگرچه تعداد حملات خودی ممکن است کمتر از تعداد حملات غیر خودی باشد اما میزان موفقیت و آسیب آنها به مراتب بیشتر و جدی‌تر از حملات غیر خودی است [۵].

پیش‌بینی و جلوگیری از حملات خودی به دلیل قانونی‌بودن فعالیت‌ها و مجوزها امری دشوار است و روش‌های معمول تأمین امنیت مانند آنتی‌ویروس‌ها و سیستم‌های تشخیص نفوذ قادر به مقابله با آنها نیستند [۲]. همان طور که اشاره شد بهترین روش برای جلوگیری از حملات خودی استفاده از مدل‌های مناسب کنترل دسترسی است. این در حالی است که در سیستم‌های اسکادا با وجود آن که اپراتورها نقش کلیدی داشته و همواره در تعاملی ضروری با سیستم هستند، مدل‌های کنترل دسترسی یا اصلاً استفاده نشده و یا به شکل محدودی مورد توجه قرار گرفته‌اند. به همین دلیل امنیت سیستم‌های اسکادا به طور جدی در معرض خطر حملات خودی بوده و این موضوع اهمیت استفاده از سیستم‌های کنترل دسترسی را در آنها نشان می‌دهد [۱۶].

۳- بسته پیشنهادی مدل کنترل دسترسی

ساختار کلی بسته پیشنهادی بر پایه مدل استاندارد RBAC بوده و در آن علاوه بر در نظر گرفتن ویژگی‌های مدل RBAC (مانند ارث‌بری نقش‌ها، جداسازی وظایف ایستا SSDs[4] و پویا DSDs[5] و غیره)، وابستگی‌های به زمان فعال‌شدن نقش‌ها، نوع فعالیت کاربر، وضعیت شبکه، پیام آگهی، طبقه‌بندی منابع و پویایی سطوح امنیتی لحاظ شده است. لازم به توضیح است که استفاده از مدل پیشنهادی موجب مدیریت هرچه صحیح‌تر در اختصاص نقش‌ها و مجوزها به کاربران و اجرای سیاست‌های کنترل دسترسی است و هیچ گونه تأخیری در اجرای عملیات جاری سیستم اسکادا به وجود نخواهد آورد. به عبارت دیگر با تعیین دقیق نقش‌های مجاز کاربر در هر نشست (هنگام ورود به سیستم و بعد از مرحله احراز هویت) مجوزهای مجاز کنترل شبکه در اختیار کاربر قرار خواهد گرفت.

۳-۱ نیازمندی‌ها و محدودیت‌های کنترل دسترسی در سیستم اسکادا

ارائه یک مدل جدید کنترل دسترسی منوط به شناخت کامل از نقش‌ها، منابع، نیازمندی‌ها و محدودیت‌های موجود در سیستم است. در سیستم پیچیده اسکادا به دلیل تعداد زیاد منابع، متغیرهای سیستمی فراوان و شرایط مختلف شبکه، ارائه یک مدل امن کنترل دسترسی با قابلیت انعطاف‌پذیری مناسب کاری بسیار پیچیده و مشکل است [۱۶]. در ادامه نگاهی دقیق به نقش‌ها، منابع و نیازمندی‌های کنترل دسترسی در سیستم اسکادا خواهیم داشت.

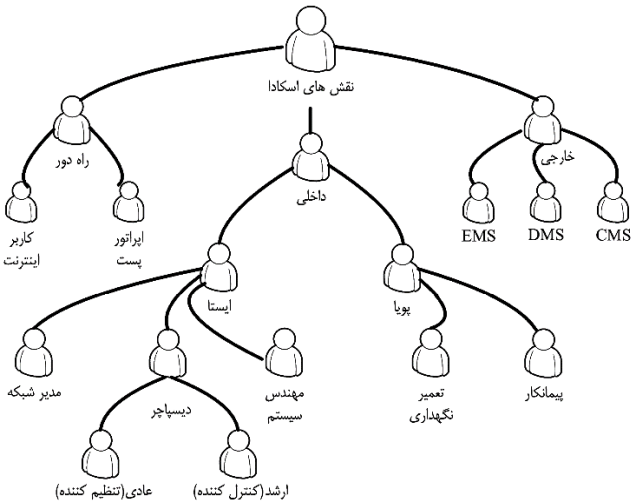
۳-۱-۱ نقش‌های اسکادا

نقش‌های اسکادا را می‌توان به سه گروه داخلی، خارجی و راه دور تقسیم کرد. شکل ۴ انواع نقش‌های اسکادا را نشان می‌دهد. نقش داخلی به دو گروه ثابت و پویا تقسیم می‌شود: گروه ثابت کاربرانی هستند که به عنوان عضو مرکز کنترل در نوبت کاری خود همیشه حضور دارند، مانند مهندس سیستم، دیسپاچرها، مدیر شبکه و غیره. گروه پویا کاربرانی هستند که به طور تصادفی در مرکز کنترل حاضر می‌شوند، مانند پیمانکاران و تولیدکنندگان انواع نرم‌افزارها و سخت‌افزارها، کاربران بخش تعمیر و نگهداری و غیره. انواع برنامه‌های کاربردی مانند EMS[6]،

1. Remote Terminal Unit
2. Human Machine Interface
3. Historian Server
4. Static Separation of Duties
5. Dynamic Separation of Duties
6. Energy Management System

www.SID.ir

Archive of SID



شکل ۴: نقش‌های سیستم اسکادا.

CMS[1]، DMS[2] و غیره که از داده‌های اسکادا برای کاربردهای خاص استفاده می‌کنند [۱۲] به عنوان کاربر خارجی اسکادا در نظر گرفته شده‌اند. نقش کاربران راه دور به دو گروه اپراتورهای داخل پست و کاربران اینترنتی تقسیم می‌شود.

۳-۱-۲ منابع اسکادا و طبقه‌بندی آنها

منابع اسکادا شامل پست‌ها و تجهیزات داخل آنها و مجموعه داده‌های جمع‌آوری شده در مرکز کنترل است. چنانچه کاربر اسکادا بتواند بدون محدودیت به تمامی منابع دسترسی داشته باشد، احتمال سوء استفاده و ایجاد یک حمله خودی در سطح کل شبکه وجود دارد. لذا یکی از نیازمندی‌های مهم در کنترل دسترسی سیستم اسکادا آن است که سطح امنیتی منابع و سطح دسترسی نقش‌ها به آنها تعیین گردد.

از آنجایی که استاندارد CIM مدلی شیءگرا برای نگهداری اطلاعات منابع اسکادا ارائه کرده است، پیشنهاد این مقاله آن است که در مدل پیشنهادی کنترل دسترسی تعیین سطوح امنیتی منابع با توجه به ساختار ارائه‌شده در همین استاندارد انجام شود.

نکته قابل توجه دیگر در تعیین سطح امنیتی منابع اسکادا، ارائه راهکاری برای طبقه‌بندی پست‌های موجود در شبکه است. این طبقه‌بندی به علت آن است که پست‌ها از اهمیت یکسانی در شبکه برخوردار نیستند. برای مثال پست‌های با سطح ولتاژ بالاتر از اهمیت بیشتری برخوردار بوده و نیاز به امنیت بیشتری دارند. پس بایستی برای هر یک از پست‌ها سطح امنیتی تعریف کرده و دسترسی نقش‌ها به پست‌ها را متناسب با آنها تنظیم کرد. به عنوان مثال ممکن است به کاربر با نقش دیسپاچر عادی تنها مجوزهای دسترسی به پست‌های تا ۶۳ کیلوولت داده شود و برای دسترسی به پست‌های با ولتاژ بالاتر نیاز به فعال‌کردن نقش‌های با سطوح دسترسی بالاتر باشد.

۳-۱-۳ تغییر سطوح امنیتی

یکی دیگر از نیازمندی‌ها در کنترل دسترسی سیستم اسکادا آن است که سطح امنیتی داده‌های جمع‌آوری شده از پست‌ها با گذشت زمان تغییر می‌کند. به این صورت که هرچه داده‌ها به زمان حال نزدیک‌ترند از ارزش بیشتر و هر چه قدیمی‌تر باشند از ارزش کمتری برخوردار هستند. برای مثال سطح امنیتی داده‌های ثبت‌شده از یک پست انتقال پس از گذشت یک دوره ۵ یا ۱۰ ساله کاهش می‌یابد. این کاهش به علت آن است که داده‌های قدیمی در حفظ پایداری فعلی شبکه تأثیر نداشته و تنها برای کاربردهای خاصی (فعالیت پژوهشی مانند بررسی حوادث شبکه و ... در زمان گذشته) می‌تواند مفید باشد. لازم به ذکر است که اطلاعات قدیمی سیستم اسکادا اگرچه از سطح امنیتی کمتری برخوردارند اما همچنان برای مهاجمین به شبکه دارای بار ارزشی هستند.

۳-۱-۴ زمان فعال‌شدن نقش‌ها

از دیگر نیازمندی‌های کنترل دسترسی در سیستم اسکادا آن است که هر کاربر با توجه به الگوی زمانی از پیش تعریف شده می‌بایست قادر به فعال‌کردن نقش خود باشد. برای مثال کاربر با نقش دیسپاچر فقط در نوبت کاری خود و کاربر با نقش خارجی تنها در ساعت اداری مجوز دسترسی به داده‌ها را باید داشته باشند.

۳-۱-۵ فعالیت‌های مجاز

از آنجا که الگوی ترافیکی سیستم اسکادا معمولاً ثابت است (به دلیل ساختار ثابت شبکه و الگوی مصرف تکراری) و فعالیت‌های مجاز آن تکرارشونده هستند [۱۷]، می‌توان تمامی فعالیت‌ها و مجوزهای لازم برای انجام آنها را از پیش تعریف کرد و دسترسی نقش‌ها به مجوزها را بر اساس فعالیت‌ها تعیین نمود. با این کار هر نقش پس از فعال‌شدن در سیستم به زیرمجموعه‌ای از مجوزهای مجاز که مطابق با فعالیت انتخاب‌شده است دسترسی خواهد داشت.

فعالیت‌های مجاز با توجه به سیاست‌های سازمانی قابل تعریف است. برای مثال در سیستم اسکادای شبکه برق به فعالیت‌های زیر می‌توان اشاره کرد: نظارت و کنترل بر شبکه، تعریف و به روز رسانی ساختار شبکه، قطع/ وصل فیدرها، افزایش و کاهش تولید، عملیات مانور و غیره.

۳-۱-۶ وضعیت شبکه

یکی از نیازمندی‌های بسیار مهم در کنترل دسترسی سیستم اسکادا، توجه به وضعیت شبکه است. همان طور که می‌دانیم شبکه تولید و انتقال نیرو می‌تواند در هر یک از وضعیت‌های عادی، هشدار، اورژانس، بحرانی، ترمیم یا بازیابی قرار گیرد. میزان کنترل و مراقبت دیسپاچر از شبکه در هر وضعیت متفاوت است. برای مثال در وضعیت اورژانس که کمترین حادثه ممکن است وسعت خاموشی را در شبکه افزایش دهد، دیسپاچر مراقبت بیشتری از شبکه باید انجام دهد. لذا لازم است در شرایط اورژانس حقوق دسترسی معمولی از اعتبار ساقط شده و حقوق دسترسی شرایط اورژانس جایگزین آن گردد. دسترسی به مجوزها در وضعیت‌های متفاوت متناسب با سیاست‌های سازمانی ممکن است سخت‌گیرانه‌تر و یا آسان‌تر در نظر گرفته شود. در هر وضعیت، دسترسی به مجوزها باید به نحوی تنظیم شوند که موازنه‌ای بین امنیت سیستم و پایداری شبکه برقرار گردد.

۳-۱-۷ پیام آگهی

به منظور بالابردن بیشتر امنیت، بهتر است تا هنگام انجام برخی فعالیت‌ها در سیستم (برای مثال فعالیت کاربران خارجی و کاربران راه دور)، یک پیام آگهی[3] برای مسئول مربوطه ارسال گردد.

۳-۱-۸ لغو دسترسی

امکان لغو دسترسی به اطلاعات در هر زمانی باید امکان‌پذیر باشد.

1. Customer Management System
2. Distribution Management System
3. Notify

www.SID.ir

Archive of SID

جدول ۱: معیار امتیازدهی پست‌های انتقال و فوق توزیع [۱۸].

ردیف	عنوان شاخص	معیار امتیاز (وزن)	وزن
۱	ظرفیت ایستگاه (مگاولت آمپر)	مجموع ظرفیت ترانس‌ها ≤ ۵۰۰ (انتقال)	۲
		مجموع ظرفیت ترانس‌ها ≤ ۵۰ (فوق توزیع)	
		مجموع ظرفیت ترانس‌ها < ۵۰۰ (انتقال)	۱
		مجموع ظرفیت ترانس‌ها < ۵۰ (فوق توزیع)	
۲	تعداد ترانسفورماتور	مجموع تعداد ترانس‌ها < ۲ عدد	۲
		مجموع تعداد ترانس‌ها ≥ ۲ عدد	۱
		کلیدخانه	۱/۵
		بدون ترانس (فوق توزیع)	۰
۳	نوع شینه‌بندی ایستگاه	چندکلیدی (یک و نیم کلیدی)	۲
		دوبل/ باس اصلی و فرعی/ مش	۱
		باس‌بار ساده/ حلقوی باز، طرح H و π	۰
۴	تعداد فیدرهای ورودی/ خروجی	تعداد < ۱۰ عدد	۲
		۱۰ ≤ تعداد < ۴ (انتقال)	۱
		۱۰ ≤ تعداد < ۲ (فوق توزیع)	
		تعداد ≥ ۴ عدد (انتقال)	۰
		تعداد ≥ ۲ عدد (فوق توزیع)	
۵	رینگ یا شعاعی‌بودن در شبکه	رینگ	۲
		شعاعی	۱
۶	اهمیت ایستگاه در شبکه	بسیار مهم (>۱۰۰۰ mV)	۰-۴
		مهم	
		معمولی (<۱۰۰ mV)	

۳-۲ مدل ترکیبی پیشنهادی

۳-۲-۱ وابستگی به زمان فعال‌شدن نقش‌ها

به منظور در نظر گرفتن زمان و نوبت کاری هنگام فعال‌شدن نقش‌ها استفاده از مدل TBAC پیشنهاد می‌گردد. برای مثال محدودیت‌های زمانی به صورت زیر قابل پیاده‌سازی می‌باشند:

۱) محدودیت زمانی با الگو: این محدودیت دارای زمان شروع، پایان و الگوی تکرار به صورت زیر است:

Enable [Role] from [Begin] to [End], [pattern]

برای مثال قاعده زمانی نقش دیسپاچر در نوبت صبح به صورت زیر است:

Enable [Dispatcher] from [9am] to [5pm], [everyday]

چنانچه دیسپاچر بخواهد نقش خود را برای مدت مشخصی (هنگام مرخصی) به دیسپاچر دیگری واگذار کند، قاعده فعال‌شدن نقش دیسپاچر جایگزین به صورت زیر خواهد بود:

Enable [Dlg-dispatcher] from [9am] to [5pm], [date1_to_date2]

۲) محدودیت زمانی برای موارد خاص: این محدودیت دارای یک زمان تأخیر و یک طول مدت است:

After [Delay] of [Role 1], enable [Role 2] for [Duration]

برای مثال قاعده زمانی فعال‌شدن نقش دیسپاچر در حال آموزش به صورت زیر است:

After [1 hours] of [Dispatcher enabled], enable [Dispatcher on training] for [4 hours]

پس از گذشت ۱ ساعت از شروع فعال‌شدن کاربر با نقش دیسپاچر، او می‌تواند نقش دیسپاچر در حال آموزش را به مدت ۴ ساعت فعال کند.

جدول ۲: طبقه‌بندی کلاس‌های مورد نیاز اسکادا در استاندارد CIM.

ردیف	گروه	کلاس‌های استاندارد CIM
۱	ساختار شبکه و تجهیزات پست‌ها	Naming, PowerSystemResource, PSRType, EquipmentContainer, Equipment, Switch, Terminal, Substation, SubControlArea ConductingEquipment, TapChanger, Bay Terminal, TopologicalIsland, Breaker, TopologicalNode, TransformerWinding, Measurement, RemoteControl, Conductor RemoteSource, BusbarSection, Connector CommunicationLink, CommunicationLink, RemoteUnit, CompositSwitch, ConductingEquipment, ConnectivityNode
۲	اندازه‌گیری و کنترل	MeasurementValue, AnalogValue, DescriteValue, Control, Command, SetPoint, AccumulatorValue
۳	پیکربندی	LimitSet, Limit, AnalogLimit, Unit AccumulatorLimit, BaseVoltage, BasePower, VoltageLevel

۳-۲-۲ نوع فعالیت کاربر، وضعیت شبکه و پیام آگهی

به منظور پیاده‌سازی وضعیت شبکه، پیام آگهی و انواع فعالیت‌های مجاز در سیستم اسکادا استفاده از مدل PBAC پیشنهاد می‌گردد. در کنترل دسترسی سیستم اسکادا از کلاس‌های Condition، Purpose و Duties به ترتیب به منظور تعریف فعالیت‌ها (خواسته‌ها)، وضعیت‌های شبکه (پیش‌شرط‌ها) و پیام آگهی می‌توان استفاده کرد.

۳-۲-۳ طبقه‌بندی منابع و تعیین سطوح امنیتی

طبقه‌بندی منابع سیستم اسکادا شامل طبقه‌بندی ۱) پست‌ها و ۲) ساختار اطلاعاتی مدل استاندارد CIM به شرح زیر قابل انجام است:

۱) طبقه‌بندی پست‌ها: پست‌های شبکه را با استفاده از ویژگی‌های آنها می‌توان طبقه‌بندی کرد. برای این منظور فهرستی از ویژگی‌های پست‌های انتقال و فوق توزیع به همراه ارزش آنها با استفاده از [۱۸] در جدول ۱ ارائه شده است. با استفاده از جدول ابتدا ارزش پست‌ها در شبکه محاسبه شده و سپس متناسب با مقدار محاسبه‌شده سطح امنیتی آنها با توجه به سیاست‌های امنیتی سازمان قابل تعیین است.

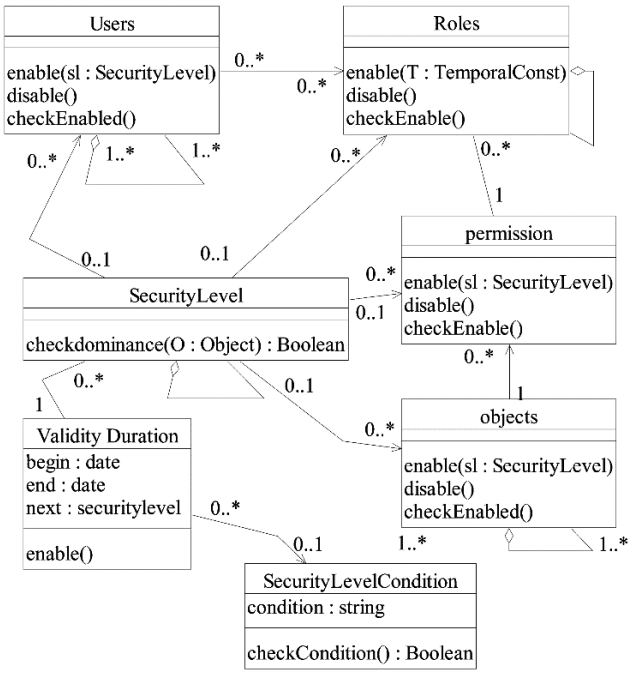
۲) طبقه‌بندی ساختار اطلاعاتی مدل استاندارد CIM: مهم‌ترین بسته‌هایی از استاندارد CIM که در نرم‌افزار اسکادا مورد استفاده قرار می‌گیرند عبارتند از Core، Topology، Measurement، SCADA و Domain. برای طبقه‌بندی کلاس‌های موجود در هر بسته می‌توان آنها را با توجه به کاربردی که در سیستم اسکادا برای آنها تعریف شده است طبقه‌بندی کرد. در این صورت هر یک از نقش‌های اسکادا با توجه به نوع فعالیتی که در سیستم دارند تنها به برخی از کلاس‌های موجود در هر بسته دسترسی خواهد داشت. جدول ۲ نحوه طبقه‌بندی کلاس‌ها را با توجه به تقسیم‌بندی زیر نشان می‌دهد:

(الف) گروه اول کلاس‌هایی را نشان می‌دهد که در رابطه با ساختار شبکه و تجهیزات پست‌ها می‌باشند. داده‌های این کلاس‌ها معمولاً در ابتدای راه‌اندازی سیستم توسط مهندس سیستم تکمیل شده و در ضمن فعالیت سیستم به روز رسانی می‌شوند. از جمله این کلاس‌ها می‌توان به کلاس‌های موجود در بسته‌های Core، Topology و SCADA اشاره کرد.

(ب) گروه دوم کلاس‌هایی را شامل می‌شود که داده‌های آنها به طور پویا در حال به روز رسانی است. این کلاس‌ها شامل مقادیر

www.SID.ir

Archive of SID



شکل ۵: نمودار کلاسی مدل DMAC پیشنهادی.

اندازه‌گیری شده از متغیرهای آنالوگ، تغییر وضعیت متغیرهای دیجیتال و دستورات ارسالی دیسپاچر است.

(ج) کلاس‌های گروه سوم شامل پارامترهای مربوط به پیکربندی تجهیزات و تنظیم مقادیر آستانه‌ای است. این پارامترها در تشخیص هشدار مربوط به مقادیر اندازه‌گیری شده و تغییر وضعیت‌های دیجیتال تأثیر مستقیم دارد.

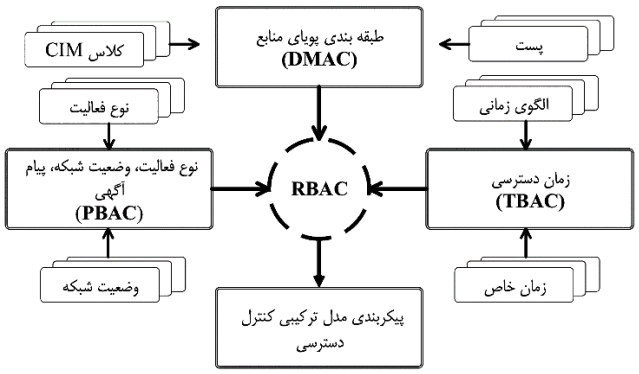
۳-۲-۴ تعیین سطوح امنیتی

به منظور پیاده‌سازی و تعیین سطوح امنیتی برای هر یک از طبقه‌های تعریف‌شده، مدل کنترل دسترسی اجباری MAC پیشنهاد می‌شود. همان طور که در شکل ۱ ملاحظه می‌شود در مدل اجباری سطوح امنیتی فقط برای کاربران و منابع قابل تعریف است.

۳-۲-۵ پویایی سطوح امنیتی

برای آن که بتوان سطوح امنیتی را در طول زمان تغییر داد لازم است تا مفهوم مدت اعتبار به مدل MAC اضافه گردد. نمودار کلاسی این مدل که با عنوان DMAC نام‌گذاری شده در شکل ۵ آمده است. در مدل DMAC با استفاده از کلاس Validity Duration برای هر سطح امنیتی یک تاریخ اعتبار و یک سطح امنیتی جدید تعیین می‌گردد. هر سطح امنیتی پس از پایان دوره اعتبار به سطح امنیتی جدید خود تبدیل خواهد شد. سطح امنیتی جدید نیز دارای دوره اعتبار است و بدین ترتیب سطح امنیتی هر موجودیت در طول زمان می‌تواند تغییر کند. برای مثال سطح امنیتی داده‌های جمع‌آوری شده از یک پست ممکن است در طول زمان کاهش یافته و برعکس سطح امنیتی کاربران پس از گذشت زمان به مرور افزایش یابد. برای تغییر سطوح امنیتی ممکن است شرایط اضافی دیگری نیز مورد نیاز باشد که توسط کلاس Security Level Condition در نظر گرفته خواهد شد.

در مدل پیشنهادی DMAC، سطح امنیتی می‌تواند به هر یک از کاربران، نقش‌ها، منابع و حتی مجوزها به طور جداگانه اختصاص پیدا کند. سطح امنیتی یک مجوز به معنای سطح امنیتی برای اجرای یک عمل بر روی یک منبع است. چنانچه یک منبع دارای سطح امنیتی باشد در این صورت برای اجرای هر عملی بر روی آن، داشتن سطح امنیتی برابر یا



شکل ۶: نمودار بلوکی مدل ترکیبی پیشنهادی.

بالاتر از آن ضروری است. چنانچه برای منبع سطح امنیتی تعیین نشده باشد و بخواهیم فقط برای اجرای برخی از توابع بر روی آن سطح امنیتی داشته باشیم، سطح امنیتی را می‌توان بر روی برخی از مجوزهای اختصاص داده شده به آن منبع قرار داد. همچنین اگر برای نقش‌ها سطح امنیتی تعریف شده باشد در این صورت سطح امنیتی کاربر، برابر با بالاترین سطح امنیتی نقش‌های اختصاص داده شده به وی در نشست جاری خواهد بود.

۳-۲-۶ مدل نهایی

در انتها با توجه به مجموعه نیازمندی‌هایی که برای سیستم اسکادا بیان شد، یک مدل ترکیبی متشکل از مدل‌های DMAC، TBAC و PBAC برای کنترل دسترسی سیستم اسکادا پیشنهاد می‌گردد. شکل ۶ نمودار بلوکی مدل ترکیبی را نشان می‌دهد. ساختار کلی این مدل بر اساس مدل استاندارد RBAC است. در این مدل محدودیت‌های زمان فعال‌شدن نقش‌ها، وضعیت شبکه، نوع فعالیت کاربر، سطوح امنیتی و پویایی آنها لحاظ شده است. شکل ۷ نمودار کلاسی مدل پیشنهادی را در قالب مدل استاندارد CIM و زبان UML نمایش می‌دهد. این مدل می‌تواند به عنوان بسته کنترل دسترسی برای سیستم اسکادا در کنار دیگر بسته‌های مدل CIM مورد استفاده قرار گیرد.

کلاس‌های Roles، Scada Objects، Access Privilege و Sessions مطابق با کلاس‌های مدل RBAC است. روابط ارث‌بری بین نقش‌ها و محدودیت‌های ایستا و پویا مطابق با مدل استاندارد RBAC قابل پیاده‌سازی و استفاده است.

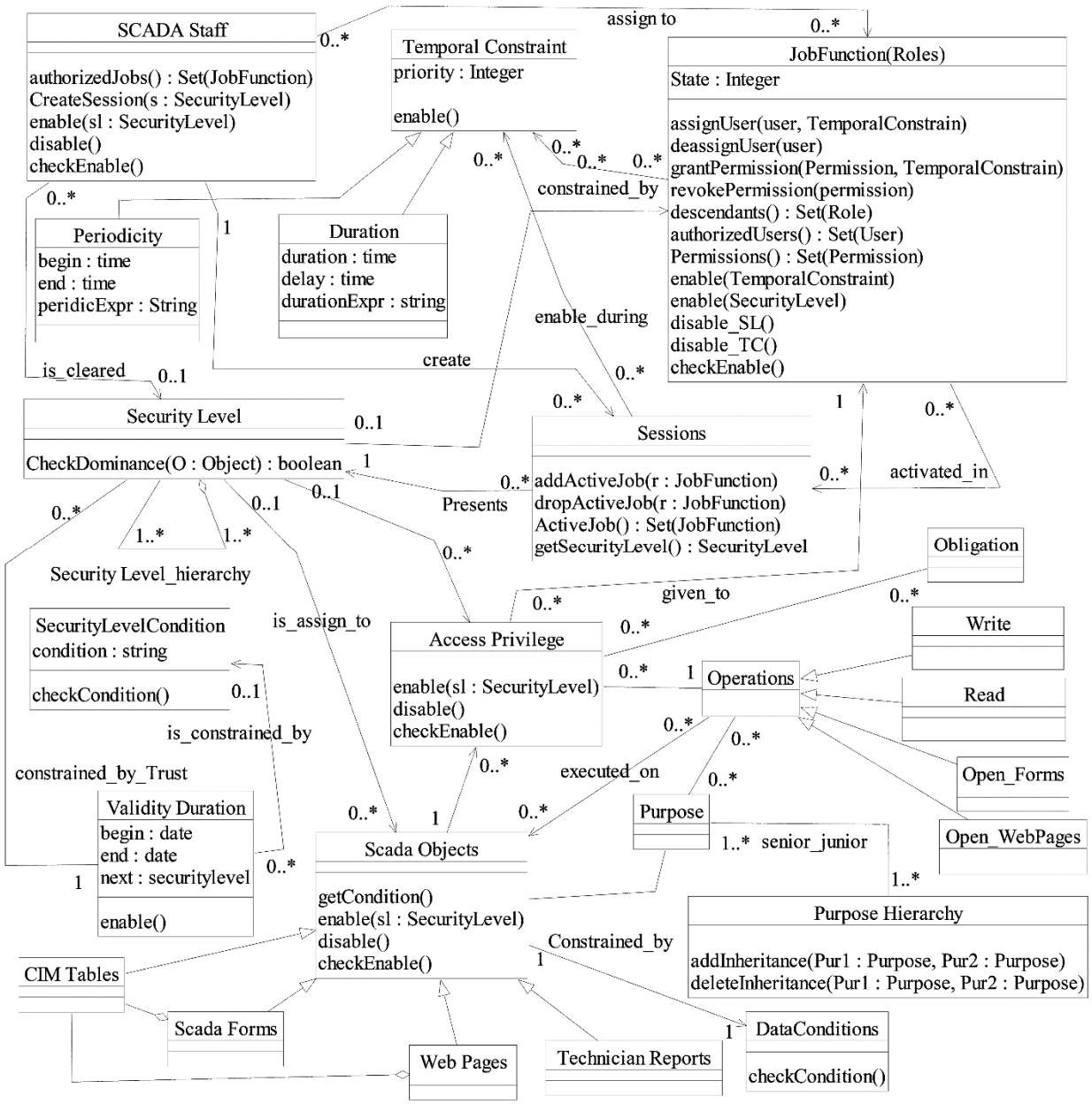
کلاس Operations شامل مجموعه فعالیت‌های سیستم اسکادا است. در این کلاس علاوه بر عملیات معمول Read و Write (خواندن و نوشتن اطلاعات موجود در کلاس‌های مدل CIM) عملیات Open_Froms و Open_WebPages (بازشدن صفحه بدون نمایش اطلاعات) هم به آن اضافه شده است. این به آن علت است که در سیستم اسکادا هر فرم یا صفحه وب علاوه بر نمایش فیلدهای اطلاعاتی می‌تواند اطلاعات دیگری که از روابط تجمع[1] و پیوند[2] بین فرم‌ها به دست می‌آید را نیز به کاربر نشان دهد. لذا کاربر مهاجم تنها با مشاهده عناوین موجود در فرم‌ها و صفحات می‌تواند به بسیاری از روابط بین داده‌ها دست یابد.

کلاس Scada Objects منابع اسکادا را شامل می‌شود. در این کلاس علاوه بر کلاس‌های مدل CIM، هر یک از فرم‌ها، صفحات وب و گزارش‌ها نیز به عنوان منبع مورد توجه قرار گرفته‌اند. کلاس‌های

1. Aggregation
2. Association

www.SID.ir

Archive of SID



شکل ۷: نمودار کلاسی مدل ترکیبی پیشنهادی.

Purpose و Purpose Hierarchy برای پیاده‌سازی فعالیت‌های مجاز، کلاس Data Conditions برای پیاده‌سازی وضعیت شبکه، کلاس‌های Temporal Constraint، Periodicity و Duration برای پیاده‌سازی محدودیت زمان فعال‌شدن نقش‌ها، کلاس‌های Security Level، Security Level Condition و Validity Duration برای پیاده‌سازی سطوح امنیتی پویا و در نهایت از کلاس Obligation برای ارسال پیام‌های آگهی قبل از دسترسی به یک مجوز استفاده شده است.

۴- آنالیز مدل پیشنهادی

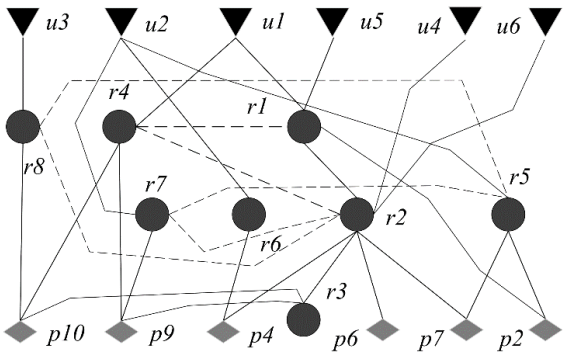
هر یک از مدل‌های استفاده‌شده در مدل پیشنهادی دارای ویژگی‌هایی هستند که ممکن است در تعامل با یکدیگر محدودیت‌هایی را برای کاربران به وجود آورند. برای مثال ممکن است در شرایط اورژانس از دسترسی کاربر به مجوزهای وضعیت اورژانس جلوگیری به عمل آید. این ممانعت از دسترسی می‌تواند به دلیل تأمین‌نشدن هر یک از ویژگی‌های دیگر (مانند زمان فعال‌شدن نقش‌ها، سطح امنیتی و ...) باشد. برای جلوگیری از چنین شرایطی باید در تنظیم قوانین کنترل دسترسی تمامی ویژگی‌ها مورد توجه قرار گرفته و دقت لازم به عمل آید. تشخیص چنین محدودیت‌های ناخواسته‌ای در قوانین کنترل دسترسی سیستم پیچیده‌ای مانند اسکادا به روش دستی و سنتی کاری مشکل و همراه با خطا است. در این مقاله از گراف کنترل دسترسی و شبکه‌های پتری رنگی به منظور آنالیز قوانین دسترسی در مدل پیشنهادی استفاده شده است. شبکه‌های پتری از ابزارهای بسیار مناسب برای بررسی رفتار سیستم‌ها در شرایط مختلف است [۱۹]. با استفاده از ابزار آنالیز فضای حالت[1] در شبکه‌های پتری رنگی با تغییر در ویژگی‌های هر یک از مدل‌ها تمامی حالت‌های ممکن در سیستم را می‌توان ایجاد کرده و بدین ترتیب مشکلات احتمالی را مورد بررسی قرار داد.

برای نشان‌دادن نحوه آنالیز قوانین کنترل دسترسی در مدل پیشنهادی از مثال جدول ۳ استفاده شده است. علایم استفاده‌شده در جدول ۳ برای انواع مجوزها، زمان‌های دسترسی، وضعیت شبکه، سطوح دسترسی، فعالیت‌های کاربران و نقش‌ها به ترتیب در جداول ۴ تا ۹ نشان داده

1. State Space Analysis

www.SID.ir

Archive of SID



شکل ۸: گراف کنترل دسترسی برای مثال جدول ۳.

جدول ۳: مثالی از محدودیت‌های کنترل دسترسی در سیستم اسکادا.

نقش	وضعیت	زمان	فعالیت	سطح دسترسی	مجوز
r_1	S_1	T_1,T_2	F_1,F_2	L_6	P_2,P_4,P_6
	S_2	T_1,T_2	F_1,F_2	L_6	P_2,P_4,P_6,P_7
r_2	S_1	T_1,T_2	F_1	L_4,L_3	P_7
	S_2	T_1,T_2	F_1	L_4,L_3	P_2,P_4,P_6
r_3	S_1	T_4	F_7	L_4,L_3	P_9,P_{10}
r_4	S_1	T_1	F_2,F_4	L_4	P_9,P_{10}
r_5	S_1	T_1	F_5	L_6	P_2,P_7
r_6	S_1,S_2	T_3	F_6	L_5	P_4
r_7	S_1	T_1	F_7	L_4	P_9
r_8	S_1	T_1	F_8	L_4	P_{10}

جدول ۴: انواع مجوزها در محدودیت‌های کنترل دسترسی.

عنوان	مجوز	عنوان	مجوز
P_1	خواندن جداول گروه ۱	P_6	نوشتن جداول گروه ۳
P_2	نوشتن جداول گروه ۱	P_7	خواندن همه گروه‌ها
P_3	خواندن جداول گروه ۲	P_8	نوشتن همه گروه‌ها
P_4	نوشتن جداول گروه ۲	P_9	خواندن اطلاعات بایگانی
P_5	خواندن جداول گروه ۳	P_{10}	گزارش از اطلاعات بایگانی

جدول ۵: زمان‌های دسترسی.

عنوان	زمان دسترسی
T_1	۸ الی ۱۶
T_2	۱۶ الی ۸
T_3	همیشه
T_4	یک ساعت بعد از فعال‌شدن

شده‌اند. شکل ۸ گراف کنترل دسترسی را با توجه به داده‌های جدول ۳ و محدودیت‌های جداسازی وظایف نشان می‌دهد. خطوط نقطه‌چین محدودیت‌های جداسازی وظایف را نمایش می‌دهند. محدودیت‌های جداسازی وظایفی که در این مثال در نظر گرفته شده‌اند عبارتند از

$$\{(r_8,r_2),(r_8,r_5),(r_4,r_1),(r_4,r_2),(r_7,r_2),(r_7,r_5)\} \quad (۱)$$

مجموعه قوانین و محدودیت‌های استفاده‌شده در این مثال را می‌توان با استفاده از تابع Chf() به صورت زیر نشان داد. تابع Chf() وظیفه بررسی ویژگی‌ها را به عهده دارد:

الف) قوانین و محدودیت‌ها در اختصاص نقش به کاربران

جدول ۶: وضعیت‌های شبکه.

عنوان	وضعیت
S_1	عادی
S_2	اورژانس

جدول ۷: سطوح امنیتی.

عنوان	امتیاز پست	سطح امنیتی
L_1	امتیاز پست ≤ ۱۵	فوق سری (C)
L_2	۱۵ > امتیاز پست ≤ ۱۲	سری (R)
L_3	۱۲ > امتیاز پست ≤ ۸	محرمانه (P)
L_4	امتیاز پست > ۸	عادی (U)
L_5	–	سطح پست مربوطه
L_6	–	همه سطوح

جدول ۸: فعالیت کاربران.

عنوان	فعالیت
F_1	نظارت بر شبکه
F_2	کنترل شبکه
F_3	تعمیر و نگهداری
F_4	نصب و راه‌اندازی
F_5	مهندسی سیستم
F_6	اندازه‌گیری
F_7	آمار و پژوهش
F_8	همکاری

جدول ۹: کاربران و نقش‌ها.

کاربر	نقش
داخلی (u_1,u_2,u_5,u_6)	دیسپاچر ارشد (r_1)
	دیسپاچر عادی (r_2)
	دیسپاچر در حال آموزش (r_3)
	پیمانکاران (r_4)
	مهندس سیستم (r_5)
راه دور (u_3)	اپراتور پست (r_6)
	کاربر اینترنت (r_7)
خارجی (u_4)	خارجی (r_8)

$$\begin{aligned}
&(u_1,r_1)\ \text{Where}\ Chf(u_1,r_1)=[T_1,S_1\ \text{or}\ S_2,F_1\ \text{or}\ F_2,L_6]\\
&(u_5,r_1)\ \text{Where}\ Chf(u_5,r_1)=[T_2,S_1,F_1\ \text{or}\ F_2,L_6]\\
&(u_2,r_2)\ \text{Where}\ Chf(u_2,r_2)=[T_1,S_1\ \text{or}\ S_2,F_1,L_3\ \text{or}\ L_4]\\
&(u_6,r_2)\ \text{Where}\ Chf(u_6,r_2)=[T_1,S_1,F_1,L_3\ \text{or}\ L_4]
\end{aligned} \quad (۲)$$

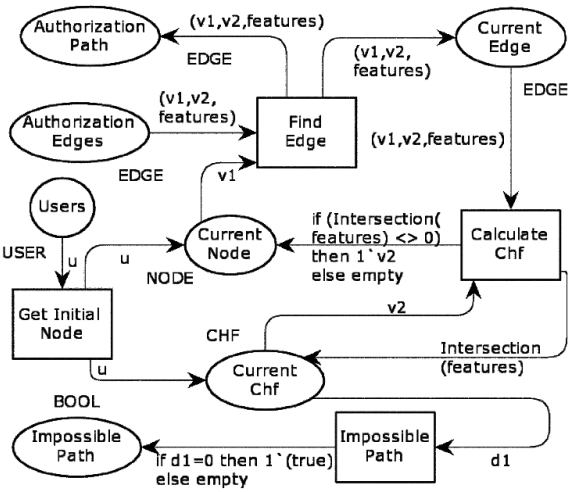
ب) قوانین و محدودیت‌ها در اختصاص مجوز به نقش‌ها

$$\begin{aligned}
&(r_2,P_7)\ \text{Where}\ Chf(r_2,P_7)=\\
&\quad[T_1\ \text{or}\ T_2,S_1\ \text{or}\ S_2,F_1,L_3\ \text{or}\ L_4]\\
&(r_1,P_4,P_6,P_7)\ \text{Where}\ Chf(r_1,P_4,P_6,P_7)=\\
&\quad[T_1\ \text{or}\ T_2,S_1\ \text{or}\ S_2,F_1\ \text{or}\ F_2,L_6]\\
&(r_2,P_4,P_6)\ \text{Where}\ Chf(r_2,P_4,P_6)=\\
&\quad[T_1\ \text{or}\ T_2,S_2,F_1,L_3\ \text{or}\ L_4]\\
&(r_1,P_2)\ \text{Where}\ Chf(r_1,P_2)=[T_1\ \text{or}\ T_2,S_2,F_1\ \text{or}\ F_2,L_6]
\end{aligned} \quad (۳)$$

ج) قوانین و محدودیت‌ها برای هر یک از مسیرهای دسترسی

www.SID.ir

Archive of SID



شکل ۹: مدل پتری رنگی برای شناسایی مسیرهای غیر ممکن.

$$
\begin{aligned}
&(u_5, P_4, P_6, P_7) \text{ Where } Chf(u_5, P_4, P_6, P_7) = \\
&\quad [T_2, S_1, F_1 \text{ or } F_2, L_6] \\
&(u_1, P_2, P_4, P_6, P_7) \text{ Where } Chf(u_1, P_2, P_4, P_6, P_7) = \\
&\quad [T_1, S_1 \text{ or } S_2, F_1 \text{ or } F_2, L_6] \\
&(u_6, P_7) \text{ Where } Chf(u_6, P_7) = [T_2, S_1, F_1, L_3 \text{ or } L_4] \\
&(u_4, P_4, P_6, P_7) \text{ Where } Chf(u_4, P_4, P_6, P_7) = \\
&\quad [T_1, S_1 \text{ or } S_2, F_1, L_3 \text{ or } L_4]
\end{aligned}
\qquad (۴)
$$

برای تشخیص مسیرهای غیر ممکن به این ترتیب عمل می‌کنیم که بر اساس گراف کنترل دسترسی چنانچه بین کاربر u، نقش r و مجوز p مسیری وجود داشته باشد، کاربر می‌تواند به آن مجوز دسترسی پیدا کند. در حالی که ممکن است در قوانین کنترل دسترسی محدودیت‌هایی وجود داشته باشد که از دسترسی کاربر به یکی از نقش‌ها یا مجوزها جلوگیری به عمل آورد. برای مثال در شکل ۸ کاربر u_4 می‌تواند به نقش r_2 دسترسی پیدا کند ولی نقش r_2 تنها در شرایط اورژانس می‌تواند به مجوزهای P_4 و P_6 دسترسی داشته باشد. لذا قوانین محدودکننده از دسترسی کاربر u_4 به مجوزهای P_4 و P_6 در شرایط عادی شبکه جلوگیری به عمل می‌آورند و بنابراین این مسیر به عنوان یک مسیر غیر ممکن برای کاربر u_4 است.

شکل ۹ یک مدل پتری رنگی برای تشخیص مسیرهای غیر ممکن در یک گراف کنترل دسترسی را نشان می‌دهد. این مدل از روش جستجو در گراف و محاسبه تابع Chf() برای هر یک از مسیرها استفاده می‌کند. چنانچه مقدار تابع Chf() با توجه به مقادیر ویژگی‌ها برای یک مسیر تهی باشد به عنوان مسیر غیر ممکن شناخته خواهد شد. آنالیز مدل از انتقال[1] Get Initial Node برای هر یک از نشانه‌ها آغاز می‌شود. تمامی یال‌های موجود در گراف کنترل دسترسی (به جز یال‌های مربوط به جداسازی وظایف) در مکان[2] AthorizationEdge و تمامی کاربران در مکان Users قرار می‌گیرند. برای هر گره v_1 یال‌های وابسته به آن توسط انتقال RetriveEdge دریافت شده و در مکان AuthorizationPath به عنوان یک مسیر ذخیره می‌گردند. سپس انتقال Calculate Chf مقدار تابع Chf() را برای آن مسیر با توجه به ویژگی‌های زمان فعال‌شدن نقش‌ها، وضعیت شبکه، نوع فعالیت کاربر و سطح امنیتی بررسی خواهد کرد. چنانچه مقدار بازگشتی تابع برای یک مسیر تهی باشد آن مسیر به عنوان یک مسیر غیر ممکن شناخته خواهد شد و سپس برای هر مسیر غیر ممکن یک نشانه در مکان Infeasible Path نگهداری می‌گردد. نتیجه آنالیز گراف شکل ۸ و نمودار فضای حالت ایجادشده دو مسیر غیر ممکن دیگر به شرح زیر است

$$
\begin{aligned}
&Authorization\ Path = \\
&\quad 1`(u_4, r_2, T_1, S_1, F_1, L_3 \text{ or } L_4, "", 0) \\
&\quad ++ 1`(r_2, p_6, T_1 \text{ or } T_2, S_2, F_1, L_3 \text{ or } L_4, "", 0); \\
&Authorization\ Path = \\
&\quad 1`(u_1, r_1, T_1 \text{ or } T_2, S_1, F_1 \text{ or } F_2, L_6, "", 0) \\
&\quad ++ 1`(r_1, p_2, T_1 \text{ or } T_2, S_2, F_1 \text{ or } F_2, L_6, "", 0);
\end{aligned}
\qquad (۵)
$$

۵- نتیجه‌گیری

این مقاله توانست با بررسی دقیق نیازمندی‌های کنترل دسترسی در سیستم اسکادا، ابتدا مفهوم مدت اعتبار سطوح امنیتی را به مدل کنترل دسترسی MAC اضافه کند (با عنوان جدید DMAC) و سپس با استفاده از مدل‌های کنترل دسترسی DMAC، TBAC و PBAC یک مدل ترکیبی و در قالب استاندارد CIM برای کنترل دسترسی سیستم اسکادا ارائه دهد. مزیت مهم مدل پیشنهادی نسبت به روش‌های قبلی آن است که از مجموعه قابلیت‌های هر یک از مدل‌های پیشین استفاده کرده و بدین ترتیب تمامی نیازمندی‌های کنترل دسترسی را در سیستم اسکادا پوشش می‌دهد. مدل ترکیبی جدید مبتنی بر نقش بوده و از وابستگی‌های به زمان فعال‌شدن نقش‌ها، وضعیت شبکه، نوع فعالیت کاربر، سطوح امنیتی و مدت اعتبار آنها پشتیبانی می‌کند. این مدل می‌تواند سطوح امنیتی پویایی را برای هر یک از منابع، نقش‌ها و مجوزها در گذر زمان تعریف کند. این مقاله توانست امنیت دسترسی را برای کلاس‌هایی از مدل CIM که در سیستم اسکادا استفاده می‌شوند، تأمین نماید. در این مقاله کلاس‌های مورد نیاز جهت پیاده‌سازی در قالب زبان UML ارائه گردید و از شبکه‌های پتری رنگی برای آنالیز محدودیت‌ها در گراف کنترل دسترسی استفاده شد.

مراجع

[1] C. Alcaraz, J. Lopez, and S. Wolthusen, "Policy enforcement system for secure interoperable control in distributed smart grid systems," *J. of Network and Computer Applications*, vol. 59, pp. 301-314, Jan. 2016.

[2] P. M. Nasr and A. Y. Varjani, "Alarm based anomaly detection of insider attacks in SCADA system," in *Proc. Smart Grid Conf. SGC'14*, 6 pp., 9-10 Dec. 2014.

[3] C. W. Ten, C. C. Liu, and G. Manimaran, "Vulnerability assessment of cybersecurity for SCADA systems," *IEEE Trans. on Power Systems*, vol. 23, no. 4, pp. 1836-1846, Nov. 2008.

[4] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," *Computers & Security*, vol. 31, no. 4, pp. 418-436, Jun. 2012.

[5] N. Baracaldo and J. Joshi, "An adaptive risk management and access control framework to mitigate insider threats," *Computers & Security*, vol. 39, pt. B, pp. 237-254, Nov. 2013.

[6] S. Kim, D. K. Kim, L. Lu, S. Kim, and S. Park, "A feature-based approach for modeling role-based access control systems," *J. of Systems and Software*, vol. 84, no. 12, pp. 2035-2052, Dec. 2011.

[7] IEC 62351-8, *Power Systems Management and Associated Information Exchange: Data and Communications Security*, International Standard, 2011.

[8] D. Rosic, U. Novak, and S. Vukmirovic, "Role-based access control model supporting regional division in smart grid system," in *Proc. Fifth Int. Conf. on Computational Intelligence, Communication Systems and Networks, CICSyN'13,* pp. 197-201, 5-7 Jun. 2013.

1. Transition
2. Place

www.SID.ir

Archive of SID

[9] H. Cheung, A. Hamlyn, T. Mander, C. Yang, and R. Cheung, "Role-based model security access control for smart power-grids computer networks," in *Proc. IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century,* 7 pp., 20-24 Jul. 2008.

[10] H. Seng-Phil, A. Gail-Joon, and X. Wenjuan, "Access control management for SCADA systems," *IEICE Trans. on Information and Systems*, vol. 91, no. 10, pp. 2449-2457, Oct. 2008.

[11] N. Slimani, H. Khambhammettu, K. Adi, and L. Logrippo, "UACML: unified access control modeling language," in *Proc. 4th IFIP Int. Conf. on New Technologies, Mobility and Security, NTMS'11,* 8 pp., Paris, France, 7-10 Feb. 2011.

[12] International Electrotechnical Commission, *IEC 61970-301, Energy Management System Application Program Interface Part 301: Common Information Model (CIM) Base*, International Standard, 2009.

[13] E. Bertino, P. A. Bonatti, and E. Ferrari, "TRBAC: a temporal role-based access control model," *ACM Trans. on Information and System Security*, vol. 4, no. 3, pp. 191-233, Aug. 2001.

[14] Q. Ni, *et al.*, "Privacy-aware role-based access control," *ACM Trans. on Information and System Security*, vol. 13, no. 3, p. 41-50, Jul. 2010.

[15] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Computers & Security*, vol. 25, no. 7, pp. 498-506, Oct. 2006.

[16] O. Rysavy, J. Rab, P. Halfar, and M. Sveda, "A formal authorization framework for networked SCADA systems," in *Proc. IEEE 19th Int. Conf. and Workshops on Engineering of Computer Based Systems, ECBS'12,* pp. 298-302, 11-13 Apr. 2012.

[17] R. R. R. Barbosa, *Anomaly Detection in SCADA Systems: A Network Based Approach*, University of Twente, 2014.

[۱۸] پ. نیرو، *استاندارد سیستم‌های اتوماسیون پست‌های انتقال و فوق توزیع*، وزارت نیرو- توانیر، ۱۳۸۶.

[19] K. Jensen and L. M. Kristensen, *Coloured Petri Nets: Modelling and Validation of Concurrent Systems*, Springer Science & Business Media, 2009.

پیام محمودی نصر تحصیلات خود را در مقاطع کارشناسی و کارشناسی ارشد مهندسی کامپیوتر به‌ترتیب در سال‌های ۱۳۷۳ و ۱۳۷۵ از دانشگاه صنعتی امیرکبیر و در مقطع دکتری مهندسی قدرت در سال ۱۳۹۵ از دانشگاه تربیت مدرس به پایان رسانده است و هم‌اکنون استادیار دانشکده مهندسی کامپیوتر دانشگاه مازندران می‌باشد. نام‌برده قبل از پیوستنش به دانشگاه مازندران در سال‌های ۱۳۷۸ الی ۱۳۸۵ به عنوان کارشناس ارشد پژوهشی در پژوهشگاه نیرو مشغول به همکاری بوده است. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: امنیت شبکه‌های صنعتی، امنیت شبکه‌های کامپیوتری، امنیت داده‌ها و شبکه‌های کامپیوتری.

علی یزدیان ورجانی تحصیلات خود را در مقطع کارشناسی مهندسی برق از دانشگاه صنعتی شریف در سال ۱۳۶۸ به اتمام رساند. ایشان مدرک کارشناسی ارشد و دکتری خود را در رشته مهندسی برق از دانشگاه ولنگونگ استرالیا به ترتیب در سال‌های ۱۳۷۳ و ۱۳۷۷ دریافت کرد. وی هم‌اکنون عضو هیأت علمی دانشکده مهندسی برق و کامپیوتر دانشگاه تربیت مدرس است. زمینه‌های تحقیقاتی مورد علاقه ایشان عبارتند از: کاربردهای الکترونیک قدرت، حفاظت و امنیت شبکه‌ها، و مدیریت امنیت اطلاعات.

www.SID.ir