عنوان مقاله: سیستم هوشمند برای مدیریت امنیت اطلاعات: مسائل مربوط به طراحی و معماری

مترجم: محمد فیض (کارشناسی ارشد مدیریت دولتی دانشگاه آزاد اسلامی واحد رشت)

موضوع: مقالات ترجمه شده / مدیریت

سال انتشار(میلادی): 2012

وضعیت: تمام متن

منبع: پایگاه مقالات علمی مدیریت www.system.parsiblog.com

منبع انتشار اصل مقاله: Issues in Informing Science and Information Technology Volume 4, 2007

تهیه و تنظیم: پایگاه مقالات علمی مدیریت www.SYSTEM.parsiblog.com

چکیده:

محدودیت های هر فناوری امنیتی به همراه رشد فشار حملات سایبر، نیاز به وجود مدیریت امنیت اطلاعات را ضروری ساخته و باعث افزایش فعالیت هایی می شود که بوسیله قسمت های از شبکه اجرایی و کارکنان امنیتی انجام می گیرد. بنابراین نیاز برای افزایش مکانیزم های ویرایش خودکار و گزارش های هوشمند برای اعتماد به سایبر وجود دارد. سیستم های هوشمند سیستم های محاسباتی خودکار بر مبنای روشهای هوشمند هستند که از مراقبت پیوسته و کنترل کردن فعالیت ها حمایت می کنند.

هوش باعث پیشرفت توانایی فردی برای تصمیم گیری بهتر می باشد. این تحقیق، ساختار مفروض یک سیستم هوشمند برای مدیریت امنیت اطلاعات (ISISM) را نشان می دهد. هدف از این سیستم بهبود بخشیدن به فرایندهای مدیریت امنیت مثل مراقبت کردن، کنترل و تصمیم گیری در ابعاد موثر می باشد که بالاتر از متخصصین در سیستم امنیتی قرار دارد و مکانیزم هایی را فراهم می کند تا باعث تقویت ساختار فعال دانش و آگاهی در مورد تهـــــــــدیدات، سیاست ها، فرآیندها و خـــــــــطرات شود. ما به مسائل مربوط به نیازها و طراحی برای اجزای اصلی سیستم هوشمند تمرکز می کنیم.

واژگان کلیدی: مدیریت امنیت اطلاعات، امنیت سایبر، سیستم هوشمند، معماری، کنترل بر مبنای عامل

مرور کلی در مورد امنیت سایبر

رشد فزاینده اینترنت، همگرایی اینترنت و برنامه های کاربردی چند رسانه ای بی سیم و خدمات ، چالش های جدید امنیتی را بوجود آورده است (Miller, 2001) .

امنیت یک سیستم پیچیده است و می بایست در همه نقاط و برای هر کاربری مورد توجه قرار بگیرد (Volonino, 2004). سازمانها نیاز به یک روش سیستماتیک برای مدیریت امنیت اطلاعات دارند که پیوستگی امنیتی را در هر سطحی نشان می دهد.

آنها به سیستم هایی نیاز دارند که از تخصیص بهینه منابع امنیتی به نسبت ریسک بیشتر و آسیب پذیری حمایت کند. بهرحال زیربنای امنیتی در بیشتر سازمانها الزامات وجود آنرا نسبت به برنامه ریزی، روش بر مبنای تعامل ، مثل مشاهده آسیب ها و استفاده از نرم افزارهای به روز(Cardoso & Freire 2005)، نشان می دهد Gordon, Loeb & Lucyshyn, 2003). از طرف دیگر برنامه های امنیتی سایبرجهت نیازهای تخصصی تر برای کامپیوتر و امنیت شبکه می باشد که به ویرایش خودکار و مکانیزم های گزارشی و تقویت محصولات برای ارزشیابی های امنیتی و مدیریت تهدیدات مورد استفاده قرار میگیرد (Chan & Perrig 2003; Hwang, Tzeng & Tsai, 2003; Leighton, 2004).

در کنار کنترل های امنیتی (سیستم امنیتی، رمزهای عبور، مشاهده تعدّی، برنامه های بازیافت حملات و ...) که وجود دارد امنیت یک سازمان شامل مسائلی است. که عموما موضوعاتی مثل سیاست ها، آموزش، عادات، آگاهی، فرآیندها و انواع دیگری از مسائل فنی و غیر فنی می باشد.(Heimerl & Voight,2005) .آموزش امنیتی و آگاهی که در مورد استفاده گسترده از زیر بناهای دیجیتالی جدید میباشد **(Tassabehji, 2005)** همه این عوامل امنیت را به صورت فرایندی در می‌آورند که بر مبنای اصول داخلی می باشد (Maiwald, 2004; Mena, 2004). چالش های موجود در مدیریت امنیت اطلاعات به همراه فقدان درک علمی از رفتارهای سازمانی نیاز به وجود سیستم های محاسباتی بهتر را باعث می شود که به طور موثر از فناوری های اطلاعاتی حمایت کنند و روشهای جدیدی که بر مبنای روشهای هوشمند و اطلاعات امنیتی می باشد برای همکاری و تقسیم اطلاعات می باشد.

سیستم های هوشمند به صورت سیستم های نرم افزاری جدید برای حمایت از برنامه های کاربردی پیچیده بوجود آمدند. در این تحقیق ما ساختاری را برای یک سیستم هوشمند برای مدیریت امنیت اطلاعات (ISISM) فرض می کنیم که از فرآیندهای امنیتی در یک سازمان حمایت می کند.

در میان این اجزا سیستم های هوشمند شامل عوامل هوشمندی هستند که سطح بالایی از خودکاری و کارکرد مناسب را نشان می دهند.دانش موجود در سیستم حمایتی این کمک را به کاربران میکند تا با سطح بالایی از دقت به فهم و حل مسائل موجود در قلمرو امنیت اطلاعات بپردازند.

بخش بعدی در این تحقیق خلاصه نتایج مربوط به مدیریت امنیت اطلاعات را نشان می دهد. یک مرور کلی در مورد تهدیدات امنیت اطلاعات که به همراه مرور روشهای AI برای برنامه های کاربردی امنیت سایبر می باشد.

سپس ساختار و اجزای اصلی سیستم هوشمند را نشان می دهیم و نیازمندیهای طراحی خاص را برای عوامل هوشمند نشان می دهیم. مسائل اصلی مرتبط با طراحی و تکنولوژی ها را با استفاده از روش مهندسی سیستم ها نشان می دهیم. ما سیستم هایی را مورد بررسی قرار می دهیم که بر مبنای کنترل بر مبنای عامل هوشمند هستند که روشی را برای تحلیل، طراحی و اجرای سیستم های نرم افزاری پیچیده ارائه می کنند. ما نتیجه گیری را بر مبنای آینده کیفی مدیریت امنیت اطلاعات و تاثیرگذاری بصورت چند مثال ادامه می دهیم.

مدیریت امنیت اطلاعات

مسائل و رویکردها

مدیریت سیستم اطلاعات زیربنایی برای اطمینان از تاثیرگذاری کنترلهای امنیت اطلاعات در طول منابع اطلاعاتی می باشد. آن مراقبت و کنترل مسائل امنیتی را نشان می دهد که برپایه اتخاذ خط مشی امنیتی ، تکنولوزی ها ، و اقدامات اصلی برای تصمیم گیری بوسیله افراد قرار دارد. هدف از مدیریت امنیت اطلاعات اطمینان از پیوستگی، اعتماد و موجودیت پذیر بودن اطلاعات در یک سازمان می باشد.

اگرچه فناوری های امنیتی مختلف از کارکردهای امنیتی خاصی حمایت می کنند مسائل دیگری وجود دارد که بر مدیریت امنیت اطلاعات تاثیر می گذارد. اینها فناوری های موثر و قابل قیاس بندی نیستند چون بر مبنای تخصص انسانی در فواصل انسانی داده ها را تحلیل می کنند. بسیاری از ابزارها و سیستم ها رخدادی را تولید می کنند و نشانه هایی را از مشکلات بوجود می آورند.

همچنین این ابزار ممکن است در زمانهای مختلف و از شرکت های مختلفی با گزارشات و توانمندیهای مختلف مدیریتی و بدتر از همه فهرستهایی از داده های مختلف بوجود بیایند. تکنولوژی های امنیتی بطور پیوسته نیستند و هر فناوری اطلاعات را با فرمت خاص خود ارائه می دهد. این سیستم ها با نسخه ها و خطوط تولید مختلف فعالیت میکنند و تمایل اندکی به اصلاح داشته و یا کارکترهایی با علامت جلوگیری از وقایع میباشند. بخش های فروش ممکن است دارای نشانه برابری نباشند. این تکنولوژی ها فاقد خصوصیات پیوستگی و تحلیل اطلاعات جمع آوری شده می باشند.

در مدیریت امنیت، تحلیلگران می بایست انتخاب کنند که چگونه بهترین مشاهدات را جمع آوری کنند و حوزه های مورد علاقه خود را جدا کنند.

بخش کوتاهی که بوسیله فناوری امنیت فراهم می شود نوع خاصی از درک مورد نیاز برای پیش بینی را فراهم می کند. سازمانها به انسانها مانند اجرا کننده شبکه یا کارمندان امنیتی نگاه می کنند که پایگاههای اطلاعاتی مختلف را برای تهدیدات جدید مورد بررسی قرار می دهند و از راه حل های ممکن برای جلوگیری از حملات استفاده می کنند .

اغلب کارمندان امنیتی مختلف مسئول مراقبت و تحلیل اطلاعات فراهم شده بوسیله یک سیستم هستند. گزارش ها نشان می دهد که کارمندان امنیتی بطور پیوسته تحلیل اطلاعات و ارائه گزارش ها را انجام نمی دهند و همه نتایج حاصل از تحلیل گزارشات را در اختیار مدیران امنیتی قرار نمی دهند. همچنین ابزار مورد استفاده بسیار محدود هستند ، چون این سیستم ها فاقد قابلیت اجرایی برای تعمیم دادن، یادگیری و تطابق در زمان هستند.

فناوری های امنیتی در حال حاضر فاقد پیوستگی، پیش بینی و بازخور زمانی به انسانها هستند و از حملات جلوگیری می کنند. همچنین فناوری ها در مقابل حملات عظیم موثر نیستند. به علاوه محدودیت های هر فناوری امنیتی به همراه رشد فشار حملات و افزایش فعالیت های این چنینی باید مورد توجه قرار بگیرند. مسائل خاص شامل جمع آوری داده، کاهش داده، نرمال کردن داده، پیوستگی رخداد، تقسیم بندی رفتار، گزارش و پاسخ است. برای فراهم کردن تصویر کامل، دقیق و جامع از رخدادهای شبکه فرایندهای بسیاری در آینده نزدیک مورد نیاز است. بنابراین راه حل های جامع مورد نیاز است که شامل مشاهده حملات منبع حمله و مشخص کردن و جلوگیری از خطر است.

نیاز برای افزایش ویرایش خودکار و مکانیزم های گزارش هوشمند وجود دارد که از ارزشیابی امنیت و مدیریت تهدیدات حمایت می کند(chang 2002) .

سیولی در مقدمه ای به گیاراتا نو و ریلی اعلام می کند که راه حل خودکارسازی منوط به کاربرد موثر از حوزه علم کامپیوتر می باشد که هوش مصنوعی نامیده میشود (Giarratano & Riley, 1989).

راه حل هایی که از تحلیل در زمان واقعی حمایت می کنند بسیار مهم هستند چون باعث می شود از بروز حملات اولیه جلوگیری شوند. این نتایج در کاهش آسیب بوجود آمده بوسیله حملات موفقیت آمیز نقش دارند و خطر از دست رفتن اطلاعات را کاهش می دهند(Kephart & Chess, 2003) . بیانیه IBM به مشکلات در مدیریت سیستم های محاسباتی اشاره می کند چون پیچیدگی آنها کارکردهای محدودی را برای انسان بوجود می آورد در حالیکه نیاز به پیوستگی و ارتباط داخلی وجود دارد.

سیستم ها حتی برای پیوند دادن سیستم فنی پیچیده هستند. مدیریت امنیت اطلاعات نیز از این قاعده مستثنی نیست. یک راه حل مفروض سیستم های محاسباتی خودکار است که خودشان می توانند مدیریت را انجام دهند.

این سیستم ها به قابلیت های اجرایی مثل تنظیم خودکار و محافظت خودکاراحتیاج دارند. متاسفانه ممکن است بوجود آوردن آن طول بکشد. در مقایسه با سیستم های خود کار روش دیگر سیستم هایی است که به تعامل موثر با عامل انسانی تاکید می کنند.

برای مثال سیاست های امنیتی می توانند اجرای عامل را کنترل کنند و با انسان ارتباط برقرار کنند تا مطمئن شوند رفتار حاصل در مقابل تهدیدها و سیاست های امنیتی به چه صورت می باشد

(Bhatti, Bertino, Ghafoor & Joshi, 2004; Bradshaw, Cabri & Montanari, 2003).

راه حل های مدیریت وقایع امنیتی مورد نیاز است تا اطلاعات تهدید آمیز را از بخشهای مختلف جمع آوری کند، وقایع ا را از چندین منبع بهم پیوند دهد و وقایع قابل توجه را مشخص کند تا خطرات مدیریت نشده را تحت پوشش قرار دهد و باعث بهبود کارکرد امنیتی شود.

نیاز به استفاده روز افزون از ابزار خودکار وجود دارد تا وقایع تهدیدات امنیتی را پیش بینی کنند. ویرایش و مکانیزم های گزارش هوشمند می بایست مدیریت را در مقیاس بزرگ و همه زمانها انجام دهد. ابزارهای خودکار کاهش نیاز به انسان را برای انجام فرآیندها بوجود می آورند.

مدیریت امنیت اطلاعات به روش مدیریت وقایع امنیتی با تقویت قابلیت های اجرایی به سازگاری و تعمیم دادن احتیاج دارد که بتواند حملات ممکن را پیش بینی کند و از فعالیت های انسانی حمایت کند.

دوود و مک هنری(۱۹۹۸) به این نکته اشاره می کنند که امنیت شبکه می بایست بهتر درک و تقویت شود و استراتژی های پیشنهادی مثل ارزش حمایت از داده ها ، درک منابع خطر ،مشکلات سیستم اداری و مهندسی اجتماعی و تجاوزات داخلی و خارجی را نیز نشان می دهند .

برای حمایت در مقابل جدیدترین نسل از تهدیدات سایبر، قوانین حمایتی پیشگیری باید مورد توجه و حمایت قرار بگیرند. تاثیرگذاری سیستم مدیریت امنیتی بوسیله سیستم هوشمند بدست می آید که بصورت توانمندی برای مشاهده. حملات ناشناخته با دقت می باشد(Wang, 2005).

تهدیدات امنیت اطلاعات

تهدیدات امنیت اطلاعات به دو گروه تقسیم بندی می شوند:(Tassabehji, 2005)

۱- منابع فنی مثل حملات بدون اجازه، مراقبت کردن، نظارت خودکار، حملات خودکار به رمز عبور ، مخفی نگهداشتن حملات.

۲- غیر فنی مثل حوادث طبیعی، حملات فیزیکی، اشتباه انسانی و مهندسی اجتماعی.

اگر سازمانها از ابزار خودکار برای تحلیل رفتار شبکه ای استفاده کنند آسیب های بوجود آمده بوسیله کرم Slammer می تواند کاهش پیدا کند تا اینکه در ژانویه ۲۰۰۳ از آن جلوگیری شد. کرم حداقل به ۷۵۰۰۰ میزبان آسیب وارد کرد و اختلالاتی را در فعالیت تجاری و روزانه بوجود آورد. (پروازهای هواپیمایی لغو شدند، اختلالات در انتخابات بوجود آمد و ماشین های خودکار بانک ها دچار عدم فعالیت شدند.)(Moore et al, 2003).

کرم به سرعت از یک شبکه به شبکه دیگر می رفت. کرم ترافیک سنگینی را در شبکه ها، مصرف پهنای باند، تجهیزات شبکه و سرور پایگاه داده بوجود آورده بود.

(CPU و حافظه) و حملات DoS داخلی شامل افزایش ترافیک چند بخشی بود. اگر همه این روندهای اندازه گیری مورد تحلیل قرار بگیرند و ارتباط آنها بوسیله ابزار هوشمند مشخص شود، آسیب بوجود آمده بوسیله این کرم می تواند کاهش پیدا کند یا از آن جلوگیری شود. ترافیک شبکه تفسیری به نگاه کردن به چیزهای مختلف احتیاج دارد و نیازمند به تحلیل منطقی اطلاعات در کوتاهترین زمان است.

مدیریت موثر امنیت اطلاعات به درک فرآیندهای اکتشافی احتیاج دارد. عموما یک حمله دارای چندین مرحله می باشد. اولین مرحله کشف یک شبکه می باشد. حمله کننده اطلاعاتی را در مورد هدف جمع آوری می کند مثل اسناد و اطلاعاتی که وجود دارند.

سپس حمله کننده تلاش می کند آسیب پذیری ها را در خدمات مشخص شده بوجود بیاورد. از این نقطه نظر اسکن ها عموما مضر می باشند بهرحال اسکن ها بخش اولیه در هر تهدید هستند. اگر مشخص شود که یک ورودی باز است هیچ ضمانتی وجود ندارد که حمله کننده باز نگردد اما بیشتر احتمال دارد که مرحله حمله را آغاز کند. چندین نوع خدمات و برنامه های کاربردی اهداف حملات هستند.

با وجود استفاده از فناوری های امنیتی بخش های اجرایی شبکه می بایست تصمیم بگیرند که چگونه از سیستم ها در مقابل حملات محافظت کنند. یک روش که شناسایی نامیده می شود بوسیله هکرها مورد استفاده قرار می گیرد تا شبکه ها را انتخاب کنند و در جستجوی اهداف برای حمله باشند. تشخیص به هکر اجازه می دهد که اهداف را مشخص کند. اهداف سیستمها یا شبکه های آسیب پذیر می باشند. برای حمایت در مقابل حملات لازم است روشهای شناسایی و دلایل آنها را بفهمیم. برای مثال با دانستن اهداف شناسایی هکر، بخشهای اجرایی شبکه و کارمندان امنیتی را مشخص کرده و امنیت شبکه را افزایش می دهند.

بنابراین مراقبت کردن و تحلیل الگوهای شناسایی هکر به درستی و پیوسته انجام می گیرد تا در مورد فشاری که به مدیریت امنیتی وارد می کنند بتوان تصمیم گرفت. در حمایت از این فعالیت ها کاربران اجرایی شبکه و بخش امنیتی روشهای موثری را برای تشخیص و تحلیل الگوهای شناسایی می توانند بوجود بیاورند.

بخش بعدی در مورد برنامه های اجرایی مختلف بر روی روشهای AI مختلف برای مراقبت، کنترل و برنامه های کاربردی امنیتی بحث می کند

روشهای هوش مصنوعی

روشهای AI (هوش مصنوعی) مثل کشف اطلاعات، شبکه های خنثی و مصنوعی، منطق پیچیده و سیستم های تخصصی می توانند به طور پیوسته به همراه روشهای فرآیندی و آماری باشند تا تحلیل و جمع آوری اطلاعات بوسیله حسگرها، الگوهای شناسایی تشخیص، رخدادهای پاکسازی و ارتباط مدیریت وقایع امنیتی و جلوگیری از تداخل ها بوجود بیاید.

این روشها باعث بهبود توانایی امنیتی سیستم های مدیریتی می شوند تا رخدادهای پاکسازی و ارتباط مدیریت وقایع امنیتی و جلوگیری از تداخل ها بوجود بیاید. این روشها باعث بهبود توانایی امنیتی سیستم های مدیریتی می شوند تا رخدادها را بهم پیوند داده و از ابزار مدرن برای مدیریت شبکه و مراقبت امنیتی استفاده کنند. روشهای آماری برای ساخت مدلهای حمایتی پیش فرض، مورد استفاده قرار می گیرند. اما این مدلها در زمینه یادگیری و به روز رسانی (Hentea, 2005a) کم فروغ هستند,(Manikopoulos & Papavassiliou, 2002).

سیستم های تخصصی، رایج ترین نمونه برای کاربر AI در تولید، ارتباطات دور برد، تجارت و سایر حوزه ها می باشد. برای مثال میکرو سیستم های خورشیدی که بوسیله سیستم اکتشافی بر مبنای میزبان بوجود آمد با استفاده از روشهای سیستم های تخصصی برای پایگاههای خورشیدی بود (Lindqvist & Porras,2001) .

سیستم ها که بر مبنای سیستم تخصصی هستند به طور کلی قابل مقیاس بندی نیستند و اساسا بر مبنای تخصص انسانی، دانستن حقایق و قوانین برای میزبان یا شبکه خاص می باشند. بهرحال سیستم های تخصصی روند جدیدی را برای پیوند دادن فرآیندهای اطلاعاتی قدیمی مثل موارد موجود در دهه ۹۰ را بوجود آوردند.

سیستم های بر مبنای اطلاعات، شبکه های خنثی و مصنوعی و منطق از مهمترین روشهای کاربردی برای برنامه های کاربردی AI می باشند که مشکلاتی مانند مراقبت از رخدادها، جدا کردن، تشخیص و کنترل سازگاری و کنترل و هدایت وجود دارد (Rodd 1992). کنترل تطابقی به قابلیت اجرایی سیستم برای تنظیم تطابق خودش برای رسیدن به حالت مطلوب دلالت دارد(Hentea, 1997;Passino & Ozguner, 1996) .

روشهای وابسته به کنترل هوشمند شامل تولید خودکار در شرکت موتور فورد میباشد (Rychtyckyj, 2005).

روشهای هوش مصنوعی باعث تقویت قابلیت های اجرایی عامل می باشند. عوامل هوشمند و سیستم های چند عامله در میان حوزه پر رشد ترین حوزه های تحقیقاتی می باشند. ارزشیابی میزان آسیب پذیری بر مبنای روشها نیز مورد بحث قرار گرفته است (Cardoso & Freire,2005). طراحی ساختار چند عامله و مسائل اجرایی برای پایگاه داده خودکار نیز توصیف شده است(Ramanujan & Capretez, 2005).

استراتژی های امنیت اطلاعات تحلیل میکنند و تکنیک هایی را برای نمایش ا طلاعاتی در خصوص بحث های مربوط به سایبر قرار میدهند(Yao, Wang, Zeng & Wang, 2005) .

یک سیستم چند عامله به چندین روش طراحی و اجرا می شود. سیستم های چند عامله برای نشان دادن مشکلات مناسب هستند و چندین روش را برای حل مشکل دارند.

عامل های هوشمند در ابتدا مناسب هستند و از لحاظ اجتماعی تعامل دارند. اگرچه روشهای بر مبنای AI برای حمایت از مدیریت امنیت اطلاعات هستند و هنوز به حوزه محدودی توجه می کنند. اخیرا روشهای AI برای بوجود آوردن سیستم های جلوگیری بکار میروند. چندین روش و مثال مورد بررسی قرار گرفته است (Hentea, 2005b) .

سیستم های هوشمند برای مدیریت شبکه از کارکردهای حمایتی مثل مراقبت، تشخیص یا مدیریت منابع شبکه خاص مورد بحث قرار گرفتند. (Berenji, 1994; Hentea, 1999; Turban, Aronson & Liang,2005).

بطور مثال نرم افزارهای محافظ بعنوان عامل امنیتی از توانایی محدود مدیریت (http://www.watchguard.com) حمایت میکنند.

شبکه های عصبی مصنوعی تکنیک هایی هستند که معتقد به تطبیق تقاضا های بیو متریک هستند. روش های شبکه های عصبی مصنوعی برای برنامه های کاربردی پیشنهاد می شوند(Kung, Mak. &Lin, 2005).

یک سیستمی که بر پایه شبکه هوش مصنوعی قرار گرفته در خصوص پوشش مدیریت دریافت اطلاعات بحث های ظریفی میکند (2005).

روشهای AI می توانند برای ساخت مدلهای هوشمند مورد استفاده قرار بگیرند تا مدیریت امنیت اطلاعات، کیفیت کارکرد و تصمیم گیری را بوجود بیاورند..(Hentea, 2003, 2004, 2005b, 2005c)

سیستم های هوشمند، کمک های هوشمند نامیده می شوند که به کاربران در فرآیند تصمیم گیری کمک می کنند و می توانند باعث شناسایی و جلوگیری از خطر سایبر شوند. مدیریت امنیت اطلاعات موثر نیاز به سیستم هوشمندی دارد که از روش مدیریت اطلاعات امنیتی با قابلیت های اجرایی، تطابق دادن و تعمیم دادن به عالیت های انسانی حمایت می کند.

بخش زیر اجزای اصلی و کارکردهای اصلی سیستم هوشمند را برای مدیریت امنیت اطلاعات (ISISM) توصیف می کند.

ساختار (ISISM)

هر سیستم هوشمند شامل دو بخش می باشد:(Meystel & Albus, 2002)

۱- داخلی یا محاسباتی که می تواند به چهار زیر شاخه هوشمند به شرح زیر تقسیم شود:

الف - پردازش حسگر_ ورودی به سیستم های هوشمند از طریق حسگرها فراهم می شود و حالت ثابتی را در دنیا بوجود می آورد. حسگرها برای مراقبت حالت دنیای خارجی و خود سیستم هوشمند مورد استفاده قرار می گیرند.

ب - مدلسازی دنیا- محاسبه حالت دنیا می باشد و شامل پایگاههایاطلاعاتی در مورد دنیا می باشد و شامل مدل شبیه سازی و محرک می باشد که اطلاعات را در مورد حالت های آینده دنیا فراهم می کند.

ج - تولید رفتار- مدل تصمیم گیری است که اهداف و برنامه ها را انتخاب می کند و دستورالعمل ها را اجرا می کند.

د - قضاوت ارزشی- هر دو حالت مشاهده و پیش بینی را مورد ارزیابی قرار می دهد و مبنایی را برای تصمیم گیری بوجود می آورد.

۲- خارجی یا وجه مشترک، ورودی و خروجی از بخش داخلی سیستم های هوشمند بوسیله حسگرها تعمیم داده می شود و می تواند در بخش های خارجی مورد توجه قرار بگیرد.

در همه سیستم های هوشمند زیر سیستم پردازش حسگر اطلاعات را از حسگر مورد نیاز بدست می آورد. سپس رفتار تولیدی زیر سیستم ها در این مورد تصمیم گیری می کند که چه فعالیتی برای دستیابی به هدف باید انجام بگیرد. رفتار تولید شده با توجه به مدل دنیای واقعی می باشد.

خروجی های موجود در سیستم های هوشمند دستورات یا عملیاتی را برای کنترل سیستم هدف بوجود می آورند. این اطلاعات مبنای اطلاعات جدید هستند و حملات سایبر را مشاهده و پیش بنی می کنند و تصمیم گیری انجام می دهند.

مثالهای این موارد شامل بخش های زیر می باشد:

- ابزاری مثل کارکرد CPU، استفاده از حافظه، استفاده از فضای دیسک، استفاده از فایل با دو رابطه، تعداد ارتباطات باز، تعداد فعالیت ها، تقاضاهای کاربری جدید، تقاضاهای نرم افزاری جدید، پایانه کاربری، زمان پاسخ، تعداد کاربرانی که در یک زمان به سیستم احتیاج دارند، تعداد کاربران در حال حاضر، تغییرات پیکربندی، دستیابی به فایل بوسیله هر کاربر، تعداد تماس های سیستم، تعداد هشدارها، شکست های کاربری، ارتباطات نیمه، دوره های خارج زمانی، زمان اجرای برنامه ها، استفاده از فایل های سیستم، کتابخانه مشترک، پروتکل های همزمان سازی، ساعت سیستم، دستیابی های کاربر به اطلاعات و فایل های اجرایی، اندازه فایل های ثبتی و...

- شبکه هایی مثل پهنای باند موجود، تاخیر، تقاضاهای دستیابی به شبکه، تعداد منابعی که برای چندین وقت موجود نیستند، تقاضا برای پروتکل جدید، تعداد ورودی هایی که همزمان باز هستند، تعداد معاملاتی که در اینترنت انجام می گیرند، تعداد تغییرات شکل بندی، صدای زیاد در مورد انتقال دوباره، تعداد دسته ها، پیام های ایمیل، پیامهای مشاوره و...

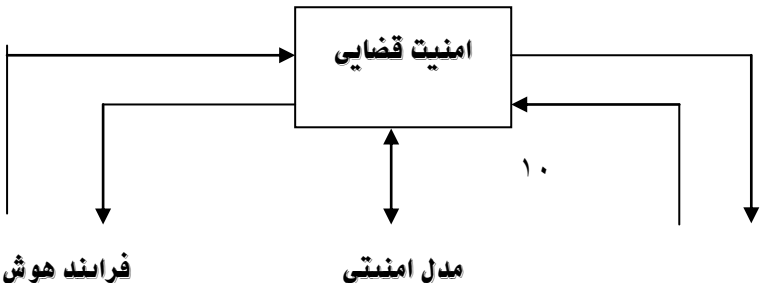
- وجوه مشترک مثل میزان استفاده آمارها
- محیط (دما، باز بودن در، بسته بودن در، علایم هشدار)
- بخش های امنیتی (سیستم های مشاهده، نرم افزار آنتی ویروس، شبکه خصوصی مجازی، مثل تعداد ارتباطات انکار شده، تعداد هشدارها، تعداد نرم افزارهای به روز شده، فعالیت های اکتشافی، تعداد کلیدهای از بین رفته، دستیابی به راه دور و...)
- سیاست های امنیتی (تاریخ موضوعی، تاریخ تغییرات، اهداف و ...)
- خطرات (پذیرفته شده، کاهش پیدا کرده، انتقال پیدا کرده)
- احتمال و برنامه های بازیابی
- امنیت و فعالیت های اجرایی شبکه (دخول به سیستم، تغییرات پیکربندی، نصب نرم افزار، به روز در آوردن نرم افزار، آزمایش کردن تعداد پیام ها، اجرای برنامه های کاربردی و...)

ما ساختار سیستم را بر مبنای روشهای سیستم کنترل واقعی (RCS) به روز در آوردیم(Meystel & Abus 2002) مسیتل و آلباس به این نکته اشاره کردند که هوش سیستمی بوجود (2002, p. 19) آمده از ساختار محدود می باشد که کارکردهای ابزارهای هوشمند را به یکدیگر ارتباط می دهد.

همه اجزای هوشمند بر مبنای کارکرد اولیه هستندکه جریانهای اطلاعاتی را بوجود می آورند. شکل (۱) نشان دهنده اجزای اصلی در بخش امنیتی می باشد. عامل دارای مفاهیمی که از طریق حسگر وارد می شوند می باشد که به عنوان ورودی در نظر گرفته می شود و فعالیت ها به عنوان خروجی هستند. عوامل نرم افزاری واحدهای محاسبای هستند که زمانهای بسیار زیادی در سیستم هوشمند در سطح مختلف تکرار می شوند همینطور که واحدها به بخش های مختلف اتصال پیدا می کنند.

در هر شیار پردازش حسگرهای امنیتی و مدلسازی امنیتی پایگاه اطلاعاتی را با گروهی از مشخصات بوجود می آورد. در هر سطحی برنامه ها آماده و به روز می شوند. ساختار یک سیستم هوشمند ساختاری خاص با عوامل است و هر عامل دارای ساختار مخصوص به خودش می باشد.

در هسته سیستم هوشمند مفهوم عامل کلی شده وجود دارد. عوامل با کارکردهای یکسان می توانند در گروهها مورد استفاده قرار بگیرند. بعدا عوامل گروهی می توانند به هم بچسبند تا گروه کلی تری را بوجود بیاورند و این فن به مدیریت اطلاعات امنیت کمک می کند. (Meystel & Abus 2002)



شکل ۱ : محتوای بخش و بروز رسانی از **(Meystel & Albus, 2002)**

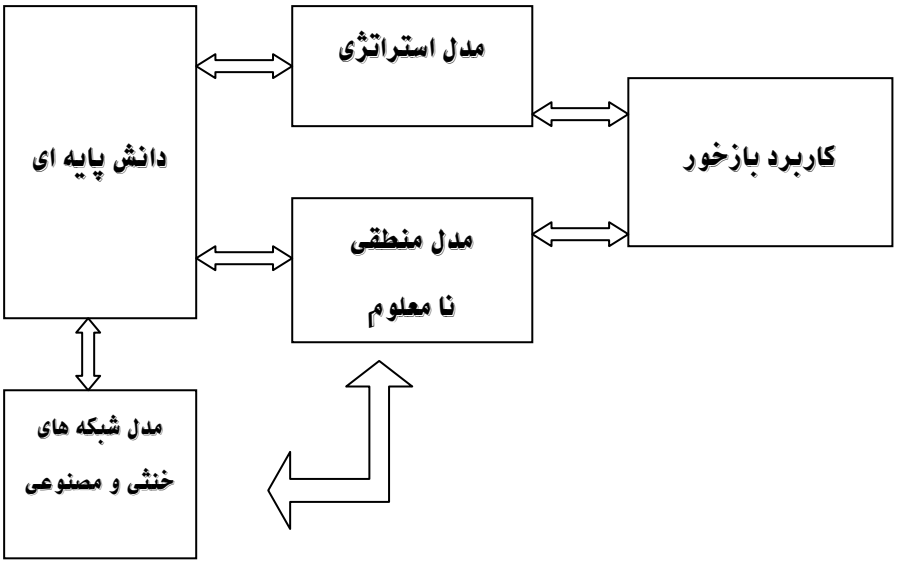
عوامل نرم افزاری می توانند مکان خود را در سیستم تغییر دهند که عوامل محرک نامیده می شوند. عوامل می توانند در طول شبکه حرکت کنند و وظایف خود را نسبت به سایر ماشین ها انجام دهند.

همچنین فرایند حرکت در سیستم های فایل، سرویس های اطلاعات و سایر عوامل انجام می گیرد. عوامل محرک برای کشف خدمات شبکه در محیط ها مورد استفاده قرار میگیرند..(Kopena et al, 2005).

فضاهای هوشمند بر مبنای ابزارهای هوشمند در بخشهای هوشمند، محل های کار، کلاس ها، بیمارستان ها و سرویس‌های حمل و نقل مورد استفاده قرار می گیرند..(Yang & Wang, 2005).

ساختار فرض شده شامل اجزای هوشمند برای بوجود آوردن رابطه های کارکردی و جریان اطلاعاتی بین زیر مجموعه های مختلف می باشد. اجزای هوشمند بر مبنای اجزایی با استفاده از یک یا چند روش AI می باشد: پردازش زبان خنثی، شبکه های عصبی مصنوعی، منطق پیچیده. به علاوه فواید رشد سیستم هوشمند را در ترکیب روش های AI و سایر فناوری ها مثل برنامه ریزی قراردادی و بسته های آماری مشاهده می کنیم که دارای ساختار سیستم هوشمند پیوندی می باشند. .(Zahedi, 1993).

شکل (۲) نشان دهنده ساختار مفروض سیستم کمکی هوشمند می باشد که بر مبنای روشهای آماری سنتی و روشهای AI مختلف می باشد که از سیستم کلی حمایت می کند که بطور خودکار و سازگار فعالیت می کند.



شکل ۲ : مدل امنیتی شرکتها

ساختار سیستم بر مبنای روش پیوندی تصمیم گیری را با استفاده از سیستم های هوشمند انجام می دهد. این سیستم با هدف بهبود بخشیدن به فرایندهای تصمیم گیری در ابعادی موثر می باشد که بالاتر از تخصص امنیتی قرار می گیرد. به علاوه این سیستم مکانیزم هایی را برای ساختار فعال آگاهی در مورد تهدیدات سیاست ها، فرآیندها و خطرات بوجود می آورد.

مدل تطابقی و حمایت کننده از طبقه بندی رویدادها و اطلاعاتی می باشد که حملات را پیش بینی می کند. یکی از اصلی ترین اجزا در طراحی رشد مدل هوشمند برای تحلیل و پیوستگی رخدادها در زمان واقعی می باشد تا حمایت و امنیت افزایش پیدا کند: سیستم های مشاهده، دیواره های امنیتی، نرم افزار آنتی ویروس، فیلترهای پاک کننده .بطور مثال مدل های نامعلوم و مصنوعی باید بروز رسانی و حمایت کند از فرایندهای طبقه بندی رویدادها و اطلاعات که در بازخورد استفاده دارد.

مدلها باید به صورتی گسترده شوند که ورودی برنامه های امنیتی و اندازه گیری هایی برای مراقبت شبکه ای، ویرایش، کنترلهای دستیابی منطقی و فیزیکی وجود داشته باشد(Hentea,2006) . مدلها باید وظایف حمایتی برای مدیریت امنیت اطلاعات مثل مشاهده کردن و کشف تهدیدات و جلوگیری از حملات بوسیله فعالیت های مجاز را داشته باشد.

نتایج در سایر بخش ها نیز می توانند مورد استفاده قرار بگیرند که در شکل(۱) نشان داده شده است. هر جزء ممکن است شامل ۱ یا ۲ مدل از شکل (۲) باشد. اطلاعات از مدلسازی امنیتی عبور می کند و اطلاعاتی را در مورد پایگاه داده

بوجود می آورد. سیستم پیوندی بخش پیوسته ای از مدلهای مختلف برای مدیریت رخداد امنیتی می باشد که شامل روشهای AI و سایر روشها می باشد که بر مبنای روش فرآیندی سنتی و آماری می باشند.

نظر اصلی در مدلهای چند گانه برای کارکردی مجزا در اندازه گیری های مختلف می باشند که برای تقسیم بندی کردن الگوهای شناسایی مورد استفاده قرار می گیرند.چون خروجی مدلها نامطمئن هستند مدل تخصصی منطق پیچیده می تواند باعث بهبود نتایج شود.

سیستم می بایست همچنین کارکردهایی برای وظایف خودکار مثل جمع آوری داده، کاهش داده، پالایش و فناوری های چند عامله داشته باشد. عوامل هوشمند از اندازه گیری های امنیت اطلاعات، مراقبت تحلیل و کنترل حمایت می کنند. سیستم ممکن است دستوراتی را برای کاربر نهایی تنظیم کند تا به ابزار دیگری برود وقتیکه نشانه های مشکوکی مشاهده می شود.

دووی و راماچاندران سیستم چند عاملی را برای مدیریت شبکه تعریف کردند که در آن عوامل مذاکراتی را انجام می دهند. این مبنای اطلاعاتی می بایست سازگار و مطابق با تصمیم گیری های کامپیوتری باشد که با مقایسه تصمیمات متخصصان انجام می گیرد. به علاوه روشهای خودکار برای کشف حقیقت، این روش ساختاری را برای تصمیم گیری و فعالیت با استفاده از تجربه انسانی بوجود می آورد.

مدل بازخور کاربرد بازخورهای مختلف را برای اجرا در شبکه یا برای گروه امنیتی بوجود می آورد. نوع بازخور نیز مهم است. بازخور مستقیم اطلاعات خاصی را در مورد نتایج و فشار ممکن در هر مورد بوجود می آورد. بازخور غیر مستقیم در سطح بالاتری قرار دارد و هیچ اطلاعات خاصی در مورد آن وجود ندارد.

این جنبه مهمی از یادگیری ماشینی می باشد. بیشتر تحقیق یادگیری ماشینی به یادگیری توجه می کنند تا بوجود آوردن بازخوردی که برای تصمیم گیری مفید می باشد. این شرایط به آسانی می توانند در برنامه ریزی ماشینی مورد استفاده قرار بگیرند تا از کاربر حمایت کنند. به علاوه برنامه یادگیری ماشینی می بایست از مبنای دانش حمایت کند تا محیط یادگیری غنی تری را بوجود بیاورد.

مسائل مربوط به طراحی

بخش اصلی تصمیم در هنگام طراحی ساختاری این است که چه عواملی می بایست در آن وجود داشته باشند. چندین عامل می توانند طراحی شوند تا از مدیریت امنیت اطلاعات محافظت کنند(Russell &Norvig) . 2003در سیستم مفروض عوامل اصلی می بایست عامل تصمیم گیرنده و کنترل کننده باشند .

یک عامل هوشمند به صورت مجموعه ای از کارکردها و قابلیت های اجرایی هوشمند مشاهده می شود. توانایی برای فعالیت کردن در محیط نامطمئن، یادگیری، سازگار پذیری، احتمال موفقیت، کارکردها چیزهایی هستند که بوسیله نگاه به مجموعه ای از کارکردها تعیین می شوند.

اگرچه گفتگوی زیادی در مورد اینکه چه چیزهایی یک عامل را تشکیل می دهد وجود دارد و اینکه کدام خصوصیات مهم است. با توجه به پیچیدگی وظایف مدیریت امنیت اطلاعات، سیستم مفروض بر مبنای پیوستگی انواع مختلفی از عوامل هوشمند و ساختار پیوندی در شرایط واقعی با محدودیت روبرو می باشد. عوامل هوشمند باعث بهبود کارکرد اجرایی شبکه می شوند. طراحی و برنامه ریزی عوامل می بایست باعث حداکثر کردن کارکرد شود (Russell & Norvig,2003).

سایر مسائل مهم مورد نیاز ورودی پذیری، پایداری، حالت ارتجاعی و امنیت عوامل و سیستم می باشد. (Bradshaw et al, 2001; Hamidi & Mohammadi, 2006).

وجه مشترک می بایست خصوصیات هوشمندی را نشان دهد که به کاربر در تصمیم گیری و کنترل فرایند امنیتی کمک کند. ارزیابی های کارکردی می بایست بر طبق نیازهای محیط مدیریت اطلاعات طراحی شود.

به علاوه مرحله طراحی باید نوع بازخور را برای یادگیری مشخص کند چون معمولا عامل بسیار مهمی در تصمیم گیری در مورد ماهیت مسئله یادگیری می باشد که عامل با آن روبرو می شود. حوزه یادگیری ماشینی معمولا بین موارد مختلف یادگیری تفاوت قائل می شود حوزه مدیریت امنیت اطلاعات گسترده است و به استفاده از یک یا مجموعه ای از شکل ها برای بهتر نتیجه گرفتن احتیاج دارد.

خصوصیت دیگر این است که تحرک پذیری را باید مورد توجه قرار دهد که تصمیم بگیرد کدام عامل در حال حرکت کردن است. به علاوه نشان دادن داده های ورودی مدل ها برای یادگیری و خروجی مدلها نقش مهمی را در طراحی ایفا می کند. عامل دیگر در طراحی موجودیت پذیری را برای تعدادی از وظایف مورد توجه قرار می دهد. اکثریت یادگیری با آگاهی در این مورد آغاز می شود که در تلاش برای یادگیری کدام عامل هستیم.

کارکردهای نشان داده شده بوسیله هر جز بر مبنای روش رشد فضایی گسترش پیدا می کند. قابلیت های اجرایی ISISM بر مبنای نیازهای امنیتی هر سازمان می باشد. ترتیب اجزای مدلها وابسته به منابع و نیازها می باشد. موارد زیر توصیف خلاصه و واضحی از خصوصیات مورد استفاده در هر پروژه می باشد:

۱- حمایت از اطلاعات با تحلیل خودکار و تفسیر داده ها و وقایع که از محیط های مختلف جمع آوری می شوند مثل کشف موارد وابسته در میان داده ها و اطلاعات و بازخور به کاربر انسانی است. مثالهای استفاده از روشهای کشف نیز مورد بحث قرار گرفته است (Hentea, 2004; Ibrahim, Folorunso & Ajayi, 2005).

۲- شبکه های عصبی مصنوعی از تقسیم بندی، وابستگی، و پیش بینی حملات سایبر در آینده حمایت می کند که بوسیله یادگیری و تطابق پذیری با اطلاعات گذشته و حال باشد. برای مثال الگوهای شناسایی می توانند با استفاده از شبکه های عصبی بر مبنای یادگیری بدون نظارت تقسیم بندی می شوند(Hentea, 2005b, 2005c) .

۳- منطق پیچیده به پردازش متغیرهای کیفی و دلیل یابی بصورت تقریبی اجازه می دهد وقتیکه پیش فرض هایی انجام می گیرد. یک مدل برای ارزشیابی ریسک مورد استفاده قرار گرفته است.(Hentea,2006).

۴- کمک هوشمند و روشهای بازخور کاربر مورد بحث قرار گرفته اند.(Hentea, 1997).

۵- روشهای آماری مورد بحث قرار گرفته اند..(Hentea, 1997, 2006)

بهرحال ارتباط بین روشهای مختلف می تواند بوجود بیاید تا تقویت جنبه های کیفی هر مدل انجام بگیرد از اینرو دانش بوجود می آید و به انسان کمک می کند تا تصمیم بگیرد.

بازده ممکن برای پیوند دادن اطلاعات شبکه های عصبی، تخصص پیچیده تلاش برای استفاده از اطلاعات و تقسیم بندی الگوهای شناسایی و خصوصیات مربوط به آن می باشد. این اطلاعات در سیستم تخصصی پیچیده می تواند مورد بحث و گفتگو قرار بگیرد و به انسان در تصمیم گیری های آینده نیز کمک کند.

به علاوه شبکه های عصبی می توانند الگوها را تشخیص داده و حملات سایبر را پیش بینی کنند. همچنین شبکه های عصبی می توانند نتایجی را از داده های نامطمئن در مورد یک وضعیت بدست بیاورند. به علاوه تبدیل دانش، نشان دادن دانش و کشف دانش اجزای اصلی در سیستم مدیریت دانش می باشند.

نیازمندی دیگر هزینه رشد و نگهداری می باشد. تیم می تواند از لحاظ هزینه موثر باشد بطوریکه استفاده سازمان از تکنولوژی های پیشرفته را تحت تاثیر قرار می دهد. کشف داده، شبکه های عصبی مصنوعی، منطق پیچیده و مبنای دانش که برای محافظت و جلوگیری می باشد (Wallich, 2003).

اگرچه چندین نوع قابلیت اجرایی را برای سیستم توضیح دادیم لیست گسترده ای از نیازمندی ها فراهم نکردیم. هدف از این تحقیق فراهم کردن ساختاری برای طراحی یک سیستم هوشمند برای مدیریت امنیت اطلاعات بود. سیستم های هوشمند مشابه برای تولید مورد بحث قرار گرفته اند(ISAM,2007) .

نتیجه گیری

روشهای واقعی پیشرفت بر مبنای مدلسازی تحلیل حسگر و عوامل هوشمند به همراه فرایندهای سنتی و روشهای آماری می توانند تشخیص، پالایش و ارتباط رخدادها را انجام داده که بوسیله منابع و حسگرهای مختلف دریافت می شوند. این روشها از قابلیت اجرایی حمایت می کنند و بازیافتی را برای اصلاح مشکلات بوجود می آورند که شامل ابزار مفیدی برای فعالیت های انسانی و جلوگیری از حملات در حال انجام می باشد.

ما ساختار جدیدی از سیستم هوشمند را برای مدیریت امنیت اطلاعات معرفی کردیم. ساختار مفروض بر مبنای چندین مثال اصولی بود که شامل مدیریت امنیت اطلاعات، ارتباط شبکه ای خوکار، علم کامپیوتر، هوش مصنوعی، تئوری کنترل مدرن، آمارها، علوم اجتماعی، تئوری سازمانی و رفتارها، علم مدیریت، استراتژی های تجاری، تحلیل ریسک و اقتصاد بود.

هیچ روش مجزایی نمی تواند رشد تهدیدات سایبر را حل کند(Gordon, Loeb & Lucyshyn, 2006).

ما نیاز به استفاده از چندین الگو داریم تا اهداف مدیریت امنیت اطلاعات را برای سازمانهای مدرن قرن بیست و یکم فراهم کند.

بر مبنای تحقیق ساختاری در AI و سایر حوزه ها، تکنولوژی عامل هوشمند کاربرد وسیعی را در امنیت سایبر دارا می باشد. تکنولوژی عامل هوشمند بوسیله تعدادی از محققان مورد توجه قرار گرفته تا جایگزین طبیعی برای برنامه نویسی هدفمند باشد.

بهرحال مواردی با خصوصیات مجزا در حال بوجود آمدن هستند اما این اجزا به رشد و پیوستگی بیشتری نیاز دارند. سیستم ها نیاز به تطابق و قابلیت کشف و ساخت مبنای جدید برای حوزه امنیت اطلاعات دارند. کار بعدی باید جستجو در مورد مفهوم منظم باشد که همه مدلها را بهم پیوند دهد تا از مدیریت حمایت کند.

References

Berenji, H.R. (1994). The unique strength of fuzzy logic control. *IEEE Expert*, *9* (4), 4.

Bhatti, R., Bertino, E., Ghafoor, A., & Joshi, J.B.D. (2004). XML-based specification for web services document security. *IEEE Computer*, *37* (4), 41-49.

Bradshaw, J.M., Suri, N., Canas, A.J., Davis, R., Ford, K., Hoffman, R., Jeffers, R., & Reichherzer, T. (2001).Terraforming cyberspace. *Computer*, *34* (7), 48-56.

Bradshaw, J. M. Cabri, J., & Montanari, R. (2003). Taking back cyberspace. *IEEE Computer*, *36* (7), 89-92.

Cardoso, R.C. & Freire, M.M. (2005). Security vulnerabilities and exposures in internet systems and services. In M. Pagani, (Ed.), *Encyclopedia of multimedia technology and networking* (pp. 910-916). Hershey, Pennsylvania, IDEA GROUP REFERENCE.

Chan, H. & Perrig, A. (2003). Security and privacy in sensor networks. *IEEE Computer*, *36* (10), 103-105.

Chang, R.K.C. (2002). Defending against flooding-based distributed denial-of-service attacks: A tutorial. *IEEE Communications Magazine*, *40* (10), 42-51.

Devi, S.S.E. & Ramachandran, V. (2002). Agent based control for embedded applications. Retrieved December 16, 2006, from http://www.hipc.org/hipc2002/2002Posters/AgentControl.pdf

Dowd, P.W. & McHenry, J.T. (1998). Network security: it's time to take it seriously. *IEEE Computer*, *31* (9), 24-28.

Giarratano, J. & Riley, G. (1989). *Expert systems principles and programming*. Boston, Massachusetts, PWS-KENT Publishing Co.

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2003). Information security expenditures and real options: A wait-and-see approach. *Computer Security Journal*, *XIX* (2), 1-7.

Gordon, L. A., Loeb, M. P. & Lucyshyn, W. (2006). Computer and cyber security breaches: Schumpeter to the rescue. *Computer Security Journal, XXII* (4), 9-10.
Hamidi, H., & Mohammadi, K. (2006). Modeling fault tolerant and secure mobile agent execution in distributed systems. *International Journal of Intelligent Information Technologies*, *2* (1), 21-36.
Heimerl, J.L. & Voight, H. (2005). Measurement: The foundation of security program design and management. *Computer Security Journal*, *XXI* (2), 1-20.
Hentea, M. (1997). Architecture and design issues in a hybrid knowledge-based expert system for intelligent quality control. PhD Thesis, Illinois Institute of Technology, Chicago, Illinois.
Hentea, M. (1999). Intelligent approach for network management system: Architecture and design issues for ATM computer
networks. *Proceedings of 1999 Advanced Simulation Technologies Conference*, San Diego, California.
Hentea, M. (2003). Intelligent model for cyber attack detection and prevention. *Proceedings of the ISCA 12th International Conference Intelligent and Adaptive Systems and Software Engineering*, San Francisco, California, 5-10.
Hentea, M. (2004). Data mining descriptive model for intrusion detection systems. *Proceedings of the 2004 Information Resources Management Association International Conference,* New Orleans, Louisiana, 1118-1119.
Hentea, M. (2005a). Information security management. In M. Pagani, (Ed.), *Encyclopedia of multimedia technology and networking (*pp. 390-395). Hershey, Pennsylvania, IDEA GROUP REFERENCE.
Hentea, M. (2005b). Improving intrusion awareness with a neural network classifier. *Proceedings of the ISCA 14th International Conference Intelligent and Adaptive Systems and Software Engineerin*g, Toronto, Canada, 163-168.

Hentea, M. (2005c). Use of reconnaissance patterns for intelligent monitoring model. *Proceedings of the 2005 Information Resources Management Association International Conference*, San Diego, California, 160-163.
Hentea, M. (2006). Enhancing information security risk management with a fuzzy model. *Proceedings of 19th International Conference on Computer Applications in Industry and Engineering*, Las Vegas, Nevada, 132-139.
Hwang, M3-S. Tzeng, S-F. & Tsai, C-S. (2003). A new secure generalization of threshold signature scheme. *Proceedings of International Technology for Research and Education*, 282-285.
Ibrahim, S.A., Folorunso, O. & Ajayi, O.B. (2005). Knowledge discovery of closed frequent calling patterns in a telecommunication database. *Proceedings of the 2005 Informing Science and IT Education Joint Conference*, Flagstaff, Arizona, 137-148. Available at http://proceedings.informingscience.org/InSITE2005/P13f80Ibra.pdf
ISAM. (2007). An intelligent systems architecture for manufacturing (ISAM): A reference model architecture for intelligent manufacturing systems**.** Retrieved January 15, 2007, from http://www.isd.mel.nist.gov/projects/rcs/isam/ISAM_web.htm#framework
Jennings, N.R., Sycara, K. & Wooldridge, M. (1998). A roadmap of agent research and development. In N. Jennings, K. Sycara, M. Georgeff (Eds.), *Autonomous Agents and Multi-Agent Systems, 1* (1), pp. 7-38. Boston, Massachussetts, Kluver Academic Publishers.
Kephart, J.O. & Chess, D.M. (2003). The vision of automatic computing. *IEEE Computer*, *36* (1), 41-50.
Kopena, J., Sulatanik, E., Naik, G., Howley, I., Peysakhov, M., Cicirello, V.A., Kam, M., & Regli, W. (2005). Service-based computing on manets: Enabling dynamic intero-perability of first responders. *IEEE Intelligent Systems, 19* (5), 17-25.
Kung, S.Y., Mak, M.W., & Lin, S.H. (2005). *Biometric authentication.* Upper Saddle River, New Jersey, Prentice Hall Professional Technical Reference.
Leighton, F.T. (2004). Hearing on the state of cyber security in the United States government. *Computer Security Journal*, *XX* (1), 15-22.
Lindqvist, U. & Porras, P. A. (2001). eXpert-BSM: A host-based intrusion detection solution for Sun Solaris. *Proceedings of the 17th Annual Computer Security Applications Conference*, 240-251.
Maiwald, E. (2004). *Fundamentals of network security*. New York, New York, McGraw-Hill/Technology

Education.
Manikopoulos, C. & Papavassiliou, S. (2002). Network intrusion and fault detection: A statistical anomaly approach. *IEEE Communications Magazine, 40* (10), 76-82.
Mena, J. (2004). Homeland security connecting the DOTS. *Software Development, 12* (5), 34-41.
Meystel, A.M. & Albus, J.M., (2002). *Intelligent systems architecture, design, and control.* New York, New York, John Wiley & Sons, Inc.
Miller, S.K. (2001). Facing the challenge of wireless security. *IEEE Computer, 34* (7), 16-18.
Moore, D., Paxson, V., Savage, S., Shannon, C, Stanford, S., & Weaver, N. (2003). Inside the Slammer worm. *IEEE Security & Privacy, 1* (4), 33-39.
Passino, K.M., & Ozguner, U.U. (1996). Intelligent control: From theory to application. *IEEE Expert Intelligent System and Their Applications, 11* (2), 28-30.
Ramanujan, S. & Capretez, M.A.M (2005). ADAM: A multi-agent system for autonomous database administration and maintenance. *International Journal of Intelligent Information Technologies, 1* (3), 14-33.
Rodd, M.G. (1992). Real-time AI for industrial control: A review. *ICARV '92 Second International Conference on Automation, Robotics and Computer Vision*, Singapore, 36-38.

Russell, S. & Norvig, P. (2003). *Artificial intelligence a modern approach* (2nd ed.). Upper Saddle River, New Jersey: Prentice Hall.
Rychtyckyj, N. (2005). Intelligent systems for manufacturing at Ford Motor company. *IEEE Intelligent Systems, 19* (5), 16-19.
Tassabehji, R. (2005). Information security threats. In M. Pagani, (Ed.), *Encyclopedia of multimedia technology and networking (*pp. 404-410). Hershey, Pennsylvania: Idea Group.
Turban, E., Aronson, J.E. & Liang, T-P. (2005). *Decision support systems and intelligent systems* (2nd ed.). Upper Saddle, New Jersey: Prentice Hall.
Volonino, L. & Robinson. (2004). *S.R. Principles and practice of information security*. Upper Saddle River, New Jersey: Pearson Prentice Hall.
Wallich, P. (2003). Getting the message. *IEEE Spectrum, 40* (4), 39-42.
Wang, F-Y. (2005). Agent-based control for networked traffic management systems. *IEEE Intelligent Systems, 19* (5), 92-96.
Wang, W. (2005). The intelligent proactive information assurance and security technology. Retrieved on January 5, 2005, from http://security.ittoolbox.com/browse.asp?c=SecurityPeerPublishing&r=http%3A%2F%2Fhosteddocs%2Eittoolbox%2Ecom%2FIntelligentIPDMTheWinningFormula%2Epdf
Willow, C.C. (2005). A neural network-based agent framework for mail server management. *International Journal of Intelligent Information Technologies, 1* (4), 36-52.
Yang, L. & Wang, F-Y. (2005). Driving into intelligent spaces with pervasive communications. *IEEE Intelligent Systems, 19* (5), 12-15.
Yao, Y., Wang, F-Y., Zeng, D. & Wang, J. (2005). Rule + exception strategies for security information analysis. *IEEE Intelligent Systems, 19* (5), 52-57.
Zahedi, F. (1993). *Intelligent systems for business expert systems with neural networks*. Belmont, California: Wadsworth Publishing Company.

Biography

Dr. Mariana Hentea is an Associate Professor (part-time) and Consultant. Dr. Hentea has been involved in research and development of novel products based on various emerging technologies, engineered networks and security systems for telecommunications industry and government for almost thirty years. Her research focuses in computer and network security, network design and architecture, wireless technologies, and Artificial Intelligence techniques for intrusion and prevention systems, information security management, quality of service, and intelligent control. For the past five years, Dr. Hentea has been involved in security awareness education and academic curricula related to information security and networking programs.