فصلنامه پژوهش در علوم، مهندسی و فناوری
دوره ۴، شماره ۲، تابستان ۱۳۹۷
صفحات ۱-۸
ISSN: 2476-5082
www.uctjournals.com

بررسی امنیت در سیستم های اطلاعاتی توسعه یافته با روش معماری سرویسگرا(SOA)

مریم پرندوار

کارشناسی ارشد، مهندسی کامپیوتر- نرم افزار، دانشگاه آزاد علوم و تحقیقات یاسوج، یاسوج، ایران.
Email: mari.parandvar@yahoo.com

چکیده

مزایا و ویژگی های خاص معماری سرویسگرا و گسترش بهکارگیری این معماری، درعمل مباحث امنیتی مرتبط با SOAرا که در پاره ای از موارد متفاوت از اصول امنیتی سیستمهای اطلاعاتی سنتی است، به دنبال دارد. هدف از این نوشتار، بررسی ابعاد مختلف امنیتی و ارائه راهکارهایی برای امنیت در سیستمهای اطلاعاتی با معماری سرویسگرا است. امید است که نتایج این پژوهش بتواند به مدیران ITدر برقراری یک سیستم اطلاعاتی ایمن و ایمن سازی هر چه بهتر معماری سرویسگرا یاری رساند. این مقاله به طور کلی به چالشها و راهکارها در امنیت شبکه می پردازد. در ابتدای مقاله به مباحثی چون:امنیت شبکه های اطلاعاتی و ارتباطی، اهمیت امنیت شبکه، سابقهٔ امنیت شبکه، پیدایش جرایم رایانه ای، طبقه بندی جرایم رایانه ای، و راهکارهایی که برای این چالش پیشنهاد شده است از جمله کنترل دولتی، کنترل سازمانی، کنترل فردی، تقویت اینترانتها، وجود یک نظام قدرتمند و کار گسترده فرهنگی برای آگاهی کاربران و فایروالها پرداخته می شود. در آخر نیز به مسأله اینترنت و امنیت فرهنگی در ایران و چالش هایی که در این زمینه مطرح گردیده پرداخته شده و برای رفع این مشکل پیشنهاداتی نیز ارائه می گردد.

واژه‌های کلیدی: امنیت وب سرویس، سرویس، معماری سرویسگرا.

مقدمه

امنیت ، مبحثی کاملا پیچیده ولی با اصولی ساده است. در بسیاری از مواقع همین سادگی اصول هستند که ما را دچار گمراهی می کنند و دور نمای فعالیت های ما را از لحاظ سهولت و اطمینان در سایه ای از ابهام فرو می برند. باید گفت که امنیت یک پردازش چند لایه است. تعیین نوع و نحوه تلقین لایه های دفاعی مورد نیاز ، فقط پس از تکمیل ارزیابی قابل ارائه است. تهیه لیستی از سیاست های اجرایی بر مبنای اینکه چه چیزی برای سازمان مهم تر و انجام آن ساده تر است در اولویت قرار دارد. پس از آنکه این اولویت ها به تایید رسیدند هر یک از آنها باید به سرعت در جای خود به اجرا گذارده شود (یامانی و همکاران[1]،۲۰۱۰).

معماری سرویسگرا که امروزه اکثر سازمانها در سراسر جهان آن را پذیرفته اند ، توانسته است افزون بر حل برخی مشکلات، مزایای زیادی را برای سازمان ها به همراه داشته باشد؛ اما علاوه بر مزایای بی شماری که این معماری به همراه دارد، ویژگیهای خاص معماری سرویسگرا، از جمله باز بودن مرزهای آن، موجب شده تا امنیت این سیستم اطلاعاتی در مقایسه با سایر سیستم های اطلاعاتی بیشتر در معرض خطر قرار گیرد. به همین دلیل محافظت از این نوع سیستم های اطلاعاتی که یک نوع دارایی سازمان به شمار می روند، اهمیت بسیاری پیدا می کند(ایزدی،۱۳۸۹).

در همین ارتباط، هدف این پژوهش بررسی ابعاد مختلف امنیتی و ارائه راهکارهایی برای برقراری امنیت در سیستم های اطلاعاتی توسعه یافته با معماری سرویس گرا است. معماری سرویس گرا دارای ساختار توزیع شدهای است و تأکید آن بر تجزیه عملیات کسب وکاری پیچیده به اجزایی است که قابل استفاده مجدد باشد و مزایای بیشتری را از استاندارد سازی فرآیند های کسب وکاری ارائه دهد که این اجزا، همان سرویس ها هستند. به گفته ای، سرویس ها اجزای توزیع شده با رابطه ای تعریف شده هستند که پیام هایXMLرا پردازش و تبادل میکنند. یکپارچگی وتعامل بین سرویس ها از طریق فناوری وب سرویس و از طریق استانداردهایی مانند،WSDL، SOAP،UDDI انجام می شود(همار[2]،۲۰۰۶).

مهم ترین جنبه های امنیتی که باید در معماری سرویسگرا به آن توجه شود، شامل :در نظر گرفتن یک سیاست امنیتی جامع، در نظر گرفتن امنیت به منزله یک سرویس و مورد توجه قرار دادن عواملی همچون احراز هویت، کنترل دست یابی، تمامیت و محرمانگی پیام، امنیت سطح پیام، امنیت در سطح نقل و انتقال، در دسترس بودن یک سرویس یا یک درخواست، ممیزی به معنای بررسی و حسابرسی دادهها، فرآیندها، تراکنش های انجام شده در سیستم های اطلاعاتی، مدیریت کردن امنیت، مدیری تکردن سیاست، مدیریت سیاست امنیتی، نظارت و مدیریت ریسک و عوامل دیگری چون امنیت منابع انسانی، امنیت محیط و امنیت منابع فیزیکی و مانند آن می شود(سیمینگ و همکاران[3]،۲۰۱۰).

ارزیابی امنیتی یک بخش بسیار مهم تراز برنامه ریزی امنیتی است. مزایای رقابتی معماری سرویسگرا سبب رشد روزافزون این معماری، به ویژه در دو دهه اخیر در سراسر جهان شده است؛ اما ویژگی خاص معماری سرویس گرا، از جمله خاصیت توزیع شدگی و باز بودن مرزهای آن موجب شده تا امنیت این معماری با چالش هایی همچون نبودن مفهوم پیوستگی، احراز هویت برای سرویس های بیرونی، امنیت بین مرزها، امنیت برنامه های کاربردی که از ترکیب چندین سرویس تشکیل شده اند و. . . همراه باشد. گرچه هر ساله تعداد مقاله هایی که به جنبه خاصی از امنیت معماری سرویسگرا میپردازند، در حال افزایش است؛ اما به نظرمی رسد به دلیل نو پا بودن این نوع معماری و عدم شناخت بسیاری از خبرگان حوزه سیستم های اطلاعاتی و شبکه و چالش های موجود در زمینه امنیت معماری سرویس گر ا، هنوز کتاب ها و مقاله های چندانی در این زمینه تألیف نشده است. هدف این پژوهش کمک به تصمیم گیری بهتر مدیران و مجریانی است که مسئول برقراری امنیت در سیستم های اطلاعاتی با معماری سرویسگرا هستند. هدف مطالعه حاضر بررسی امنیت در سیستم های اطلاعاتی توسعه یافته با روش معماری سرویسگرا(SOA) می باشد.

[1] Yamany et al
[2] Hammar
[3] Siming et al

سابقه پژوهش

در تحقیق مقدم نژاد در سال ۱۳۹۱، ابتدا، چارچوب بعضی از آسیب های امنیتی حوزه فن آوری اطلاعات با ذکر مصادیقی از انواع حملات انجام شده به شبکه های رایانه ای، تبیین شده است. سپس آسیب های امنیتی فن آوری اطلاعات در حوزه های جمع آوری، پردازش، ذخیره سازی و انتقال اطلاعات استخراج گردیده است و سرانجام عوامل موثر بر آن بیان شده است. داده های این پژوهش با استفاده از آمار توصیفی (شامل میانگین، واریانس، انحراف معیار) و آمار استنباطی (شامل تحلیل عوامل، آزمون آماره استنباطی، آزمون فریدمن با استفاده از نرم افزار SPSS) مورد تجزیه و تحلیل قرار گرفته است. اعتبار پرسشنامه از طریق به دست آوردن ضریب آلفای کرانباخ با استفاده از نرم افزار SPSS صورت گرفته است. بومی سازی سامانه های فن آوری اطلاعات به معنای واقعی با رویکرد تاکتیک های نوآوری و خلاقیت در این حوزه، کنترل فریب سایبری حریفان، کنترل ساختاریافته دقیق فضای انتقال اطلاعات و همچنین تبیین سناریوی چگونگی پردازش اطلاعات حریفان در آینده، از نتایج مهم این پژوهش است.

در مطالعه توسط تقوا و ایزدی در سال ۱۳۹۲ در رابطه با بررسی امنیت در سیستم های اطلاعاتی توسعه یافته با روش معماری سرویسگرا بعد از استخراج مهم ترین شاخص ها، از نمونه آماری در این باره پرسش بعمل آمد. پس از گردآوری دادهها با کمک آزمون تی، به تجزیه و تحلیل آنها پرداخته شد. سپس با کمک تحلیل سلسله مراتبی دادهها، مهم ترین ابعاد امنیتی و زیر ابعاد مربوط به هریک، به ترتیب اهمیت اولوی تبندی شدند. هدف از این نوشتار ، بررسی ابعاد مختلف امنیتی و ارائه راهکارهایی برای امنیت در سیستم های اطلاعاتی با معماری سرویس گرا است. در برقراری یک سیستم اطلاعاتی ایمن و ITامید است که نتایج این پژوهش بتواند به مدیران ایمن سازی هر چه بهتر معماری سرویسگرا یاری رساند. پژوهش حاضر از دید هدف کاربردی و از دیدگاه روش انجام پژوهش ، توصیفی شمرده می شود.

به طور کلی در مدل امنیت به منزله یک سرویس، منطق امنیت به صورت بخشی از یک کاربرد یا بخشی از منطق یک سرویس نیست، بلکه به صورت مجزا و متمرکز در یک سرویس امنیتی پیاده سازی می شود. تمامی تبادلات به صورت داده، پیام،درخواست و. . . نخست تحت کنترل و نظارت این سرویس قرار میگیرد (دارا، ۱۳۸۸).

روسادو و همکاران (۲۰۱۱) در مطالعه ای با موضوع معماری سرویسگرا برای امنیت سیستم شبکه همراه بیان کردند که امنیت در سیستم های شبکه همراه، بسیار ضروری است؛ در حالی که تأمین امنیت این سیستم ها به دلیل کمبود منابع در این دستگاهها، سخت و پیچیده است. در این پژوهش برای حفظ امنیت این سیستم ها، از مدلی بر اساس طراحی معماری سرویسگرا است فاده شده است. این مدل تا اندازه ای محدودیتهای دسترسی به امنیت شبکه های تلفن همراه را برآورده می کند؛ اما نتایج پژوهش نشان میدهد که این مدل به طور کامل راهگشا نبوده است.

اشلی وبوکر ۲۰۰۷، یک سیاست امنیتی، اهداف، محدوده امنیت اطلاعات مطلوب، اهمیت امنیت به منزله یک عامل مهم برای توسعه سازمان، پشتیبانی به منظور معرفی سیستم های امنیتی، اصول اولیه به کارگیری امنیت اطلاعات، مسئولیت که مرتبط هستند به معرفی این سیستم ها،اسناد و آیین نامه هایی برای کارمندان در رابطه با سیستم ها ی امنیتی را تعریف می کند.

معماری سرویس گرا

معماری سرویسگرا، روشی برای ساخت سیستم های توزیع شدهای است که در آنها عملکرد سیستم، به صورت سرویس در اختیار کاربران یا سایر سرویس ها قرار میگیرد. این نوع معماری به دلیل مزایای بی شمار خود، امروزه از سوی اکثر سازمان ها در سراسر جهان پذیرفته شده است. ویژگی خاص معماری سرویسگرا، از جمله باز بودن مرزهای آن، موجب شده است تا امنیت این معماری نسبت به سایر سیستم های اطلاعاتی بیشتر در معرض خطر قرار گیرد. در حال حاضر یکی از مشکلات بزرگ در گسترش این معماری، چالش های امنیتی موجود در آن است. از دسته مهم ترین جنبه های امنیتی معماری سرویسگرا مواردی است که در زیر اشاره شده است:

سیاست امنیتی:یک سیاست امنیتی، اهداف، محدوده امنیت اطلاعات مطلوب، اهمیت امنیت به منزله یک عامل مهم برای توسعه سازمان، پشتیبانی به منظور معرفی سیستم ه ای امنیتی، اصول اولیه به کارگیری امنیت اطلاعات، مسئولیت که مرتبط

هستند به معرفی این سیستم ها، اسناد و آیی ننامههایی برای کارمندان در رابطه با سیستم ها ی امنیتی را تعریف می کند (اشلی و بروکر[۴]، ۲۰۰۷).

امنیت به منزله یک سرویس:به طور کلی در مدل امنیت به منزله یک سرویس، منطق امنیت به صورت بخشی از یک کاربرد یا بخشی از منطق یک سرویس نیست، بلکه به صورت مجزا و متمرکز در یک سرویس امنیتی پیاده سازی می شود. تمامی تبادلات به صورت داده، پیام،درخواست و. . . نخست تحت کنترل و نظارت این سرویس قرار میگیرد (دارا، ۱۳۸۸).

احراز هویت:احراز هویت در شبکه های رایانه ای، بدین معناست که یک سرویس دهنده بتواند تشخیص دهد فرد یا سرویسی که تقاضایی را روی آن سیستم دارد ، مجاز است یا نه؟(دارا، ۱۳۸۸).

کنترل دست یابی:کنترل دست یابی را میتوان جلوگیری از استفاده غیرمجاز از منابع دانست. بدین معنا که چه کسی میتواند به منبع دسترسی داشته باشد، دست یابی تحت چه شرایطی می تواند انجام گیرد و کسانی که به منابع دست یابی دارند، چه کارهایی می توانند انجام دهند (دارا، ۱۳۸۸).

تمامیت و محرمانگی پیام:تمامیت پیام، تضمین میکند پیام یا دادههای دریافتی، ب هطور دقیقهمان چیزی است که از جانب نهاد مجاز ارسال شده است و فاقد هرگونه تغییر، درج، حذف یاتکرار است. محرمانگی را میتوان به معنای حفاظت اطلاعات از افشاگری غیر مجاز دانست. به گفته ای اطلاعات فقط باید برای افراد مجاز در دسترس باشد که معمولا در دو سطح پیام و نقل وانتقالات به کار برده میشود (دارا،۱۳۸۸).

در دسترس بودن:در دسترس بودن یک سرویس یا درخواست، نشان دهنده این است که آن سرویس قادر است پاسخ به یک سرویس را به موقع فراهم کند و اطمینان می دهد که زمانی که درخواست سرویس ها، در بسیاری از محیطهایSOA کلیدی است، در دسترس هستند (دارا،۱۳۸۸).

جنبه های گوناگون امنیت اطلاعات

اطلاعات از دیرباز موضوعی قابل توجه بوده است و حمایت از امنیت اطلاعات به ویژه برخی اطلاعات مهم و حیاتی همواره از اهمیت زیادی برخوردار بوده است ، ولی در واقع، مسئلهٔ نخست و مهم در فن صحیح حفظ امنیت نیست، بلکه در تعریف امنیت و نقض امنیت نهفته است. روشن است که پرداختن به مسائل صرفاً فنی این موضوع تا زمانی که مبانی امنیت به طور کلی موجود نباشد و ناقص باشد یا توافقی بر اصول آن وجود نداشته باشد، تمرکز بر امنیت فضای سایبر حتی در بهترین وضعیت قانونگذاری، مشکل مهمی را برطرف نخواهد ساخت. به همین دلیل، تمرکز بر مسائل پیش ینی حقوق امنیت اطلاعات باید پیش تر بر اصول محکم تری به نام مبانی پسینی امنیت بنا شود که اجماع نظر دولت و ملت در ذات اهداف امنیت است. بنابراین ، پرسش نخست اینکه امنیت کدام اطلاعات و براساس چه معیارهایی باید حفظ شود و ضمانت اجرای آن چیست؟

مطالعهٔ تطبیقی آثار خارجی دربارهٔ حقوق امنیت اطلاعات سایبری، در بیشتر موارد به جرایم رایانه ای و حقوق مسئولیت ختم میشود. در واقع، حقوق امنیت اطلاعات در متن قوانین جرایم رایانه ای، تحصیل دلیل، مسئولیت مدنی و حریم خصوص ی بحث شده است(میاوالد[۵]،۲۰۰۴).

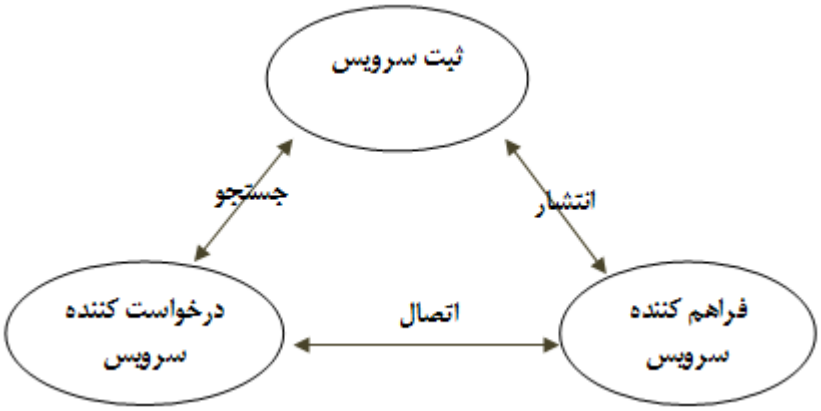
ابعاد حقوقی امنیت اطلاعات شبکه و یا حقوق مرتبط با امنیت اطلاعات شبکه به دلیل گوناگونی اصول حاکم بر آن، به سختی تن به تعریفی مشخص و قابل قبول می دهد و معمولاً به واسطهٔ شناخت پدیده های بیرونی اش به آن می شود. به دلیل همین گوناگونی، موارد ذیل به طور اجمالی توجه شده است:

امنیت در حقوق ایران به اندازهٔ کافی مدون و روشن نیست پیشینی اصول و مبانی نه تنها همهٔ جنبه های آن در قانون اساسی کشورمان ذکر نشده است ، بلکه در مرحلهٔ سیاست های کلی نظام و قوانین موضوعه، این ابهام رفع نشده است. در نتیجه نمی

[5] Miawald

توان از وضعیت فعلی، رویکردی برای قانون گذاری صحیح در عرصهٔ قانونمند ساختن جریان اطلاعات در فضای سایبر جز تا حدی در زمینهٔ اطلاعات اداری و نظامی بهره جست (جلالی فراهانی،۱۳۸۴).

هرچند توسعهٔ روزافزون فناوری اطلاعات و ظهور جامعهٔ اطلاعاتی ، دستاوردهای فوق العاده مهمی را برای بشر به ارمغان آورده است، ولی تهدیدهای بسیاری در حوزهٔ امنیت اطلاعات شبکه و سیستم اطلاعات افراد وجود دارد که مشکلات پیچیده و متعددی را به وجود می آورد. فضای سایبر بهترین مکان برای استفادهٔ مجرمین در دستیابی به اطلاعات افراد است. با توجه به اینکه اطلاعات شخصی و حتی دولتی و نظامی بسیاری در این فضا جابه جا می شود، امکان قرار گرفتن این اطلاعات در اختیار مجرمین افزایش می یابد و چون باعث تهدید امنیت جامعه و دول ت می شود ، با ابزارهای سنّتی نمی توان با آن مقابله کرد. برای رویارویی با تهدیداتی که سلامت و امنیت فضای سایبر با آن مواجه است، سه رویکرد وجود دارد که شامل جرم انگاری با توسل به قانون ؛ ایجاد قانون ویژهٔ جرایم رایانه ای و ایجاد و به کارگیری تدابیر حفاظتی و کن ترلی و پیشگیری وضعی و اجتماعی از این تهدیدات است. تدابیر حفاظتی و کنترلی نیز شامل به کارگیری فناوری های امنیت اطلاعات کنش گرایانه و واکنشی است. رویکرد پیشگیری نیز با آموزش کاربران و توانمندسازی و آگاه کردن آنها در برابر تهدیدات و همچنین به کارگیری فناوری هایی مانند رمزنگاری، دسترسی محدود و. . . امکان پذیر است. در واقع ، امنیت اطلاعات در فضای سایبر فقط در گرو همکاری متقابل همهٔ بازیگران این حوزه یعنی و ارائه دهندگان سرویس های از (ISP) کاربران اینترنت، ارائه دهندگان سرویس های اینترنتی ها و روزآمد بودن اطلاعات همهٔ این گروه ها در بارهٔ اقدامات تکنیکی و (ESP) راه دور حقوقی مرتبط با حمایت از حریم خصوصی اطلاعات در این حوزه است. علاوه بر مواردی که نقض آنها باعث مسئولیت کیفری می شود سوء استفاده از رایانه، نوع دیگری از مسئولیت وجود دارد که در نتیجهٔ سهل انگاری و بی مبالاتی به وجود می آید (عبدالهی ازگمی ،۱۳۷۵).



نمودار ۱ :مدل پایه معماری سرویس گرا

اهمیت امنیت شبکه

چنانچه به اهمیت شبکه های اطلاعاتی و نقش اساسی آن دریافت اجتماعی آینده پی برده باشیم، اهمیت امنیت این شبکه ها مشخص میگردد. اگر امنیت شبکه برقرار نگردد، مزیتهای فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوء استفاده های مادی و معنوی هستند. همچنین دستکاری اطلاعات- به عنوان زیربنای فکری ملتها توسط گروه های سازماندهی شده بین المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولتها و تهدیدی ملی محسوب می شود.

برای کشور ما که بسیاری از نرم افزارهای پایه از قبیل سیستم عامل و نرمافزارهای کاربردی و اینترنتی، از طریق واسطه ها و شرکت های خارجی تهیه می شود، بیم نفوذ از طریق راههای مخفی وجود دارد. در آینده که بانکها و بسیاری از نهادها و

دستگاه های دیگر از طریق شبکهٔ به فعالیت می پردازند، جلوگیری از نفوذ عوامل مخرب در شبکه بصورت مسئله ای استراتژیک درخواهد آمد که نپرداختن به آن باعث ایراد خساراتی خواهد شد که بعضاً جبران ناپذیر خواهد بود. چنانچه یک پیغام خاص، مثلاً از طرف شرکت مایکروسافت، به کلیه سایتهای ایرانی ارسال شود و سیستم عاملها در واکنش به این پیغام سیستمها را خراب کنند و از کار بیندازند، چه ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد؟ نکته جالب اینکه بزرگترین شرکت تولید نرم افزارهای امنیت شبکه، شرکت چک پوینت است که شعبهٔ اصلی آن در اسرائیل میباشد. مسأله امنیت شبکهٔ برای کشورها، مسألهای استراتژیک است؛ بنابراین کشور ما نیز باید به آخرین تکنولوژیهای امنیت شبکه مجهز شود و از آنجایی که این تکنولوژی ها به صورت محصولات نرم افزاری قابل خریداری نیستند، پس می بایست محققین کشور این مهم را بدست بگیرند و در آن فعالیت نمایند.

جرائم رایانه ای و اینترنتی

ویژگی برجسته فناوری اطلاعات، تأثیری است که بر تکامل فناوری ارتباطات راه دور گذاشته و خواهد گذاشت. ارتباطات کلاسیک همچون انتقال صدای انسان، جای خود را، به مقادیر وسیعی از داده ها، صوت، متن، موزیک، تصاویر ثابت و متحرک داده است. این تبادل و تکامل نه تنها بین انسانها بلکه مابین انسانها و رایانه ها، و همچنین بین خود رایانه ها نیز وجود دارد. استفاده وسیع از پست الکترونیک، و دستیابی به اطلاعات از طریق وب سایتهای متعدد در اینترنت نمونههایی از این پیشرفت ها می باشد که جامعه را بطور پیچیده ای دگرگون ساخته اند. سهولت در دسترسی و جستجوی اطلاعات موجود در سیستم های رایانهای توأم با امکانات عملی نامحدود در مبادله و توزیع اطلاعات، بدون توجه به فواصل جغرافیایی،منجر به رشد سرسام آور مقدار اطلاعات موجود در آگاهی که میتوان از آن بدست آورد، شده است.

نتیجه گیری و پیشنهادها

برای برقراری امنیت در هر سیستم اطلاعاتی، مدیران و دستاندرکاران برقراری امنیت، باید ابعاد و جنبه های مختلف امنیتی را مورد توجه قرار دهند، به گونه ای که در ایجاد یک سیستم اطلاعاتی ایمن به آنها کمک کند. در یک مقایسه کلی، تفاوت نتایج این پژوهش با پژوهش های پیشین در این است که با رویکردی متفاوت به مقوله امنیت در سیستم های اطلاعاتی با معماری سرویسگرا نگریسته شده است. این پژوهش برخلاف اکثر پژوهش ها، به جای بررسی امنیت از یک جنبه خاص و با یک رویکرد فنی، از دید سیستمی و مدیریتی به بررسی تمامی ابعاد و جنبه های امنیتی مورد نیاز یک مدیر ITکه برای برقراری امنیت در یک سیستم اطلاعاتی سرویسگرا باید مورد توجه قرار دهد با در نظر گرفتن میزان اهمیت و تأثیر هر یک، پرداخته شده است. برقراری امنیت در سطح مدیریت، امنیت در سطح معماری، امنیت در سطح شبکه و وب سرویس، امنیت در سطح برنامه های کاربردی، امنیت در سطح منابع فیزیکی و محیط، امنیت در سطح منابع انسانی و امنیت در سطح داده، می توانند به منزله ابعاد (شاخص های) اصلی چارچوب امنیتی مورد استفاده قرار گیرند. در ادامه برای بهبود در برقراری امنیت در سیستمهای اطلاعاتی سرویسگرا، راهکارهایی ارائه شده است که این راهکارها را می توان به دو دسته کلی تقسیم کرد. دسته اول راهکارهایی است که مشابه راهکارهای امنیتی در سایر سیستم های اطلاعاتی است، مانند استفاده از اصول رمزنگاری در قسمت احراز هویت یا تکثیر سرویسها برای افزایش سطح دسترسی.

دسته دوم راهکارهای امنیتی هستند که بیشتر به معماری سرویسگرا اختصاص دارند، مانند استفاده از گذرگاه سرویس سازمانی برای اجرای کنترلهای امنیتی در قسمت طراحی معماری، استفاده از WS-securityبرای امنیت سطح پیام و مانند آنها. انتظار ما بر این است که این ابعاد امنیتی و راهکارهای ارائه شده، تا اندازهای به تصمیم گیری بهتر مدیران و مجریانی مسئول برقراری امنیت در سیستم های اطلاعاتی با معماری سرویسگرا کمک کند و بتواند امنیت را در سیستمهای اطلاعاتی توسعه یافته با معماری سرویسگرا تا حد زیادی برقرار کند. با توجه به ویژگی خاص معماری سرویسگرا از جمله سیستم های توزیع شده، داشتن مرزهای باز و تعامل با سرویس های بیرونی، به تمامی مدیرانی که در این حوزه مشغول فعالیت هستند پیشنهاد می شود:

۱- در هنگام تدوین سیاست های امنیتی، به ویژه سیاستهای امنیتی مربوط به کنترل دسترسی و سیاست های مربوط به سرویسهای ترکیبی که گاهی از ترکیب سرویس های بیرونی و درونی تشکیل یافتهاند، دقت و توجه کافی داشته باشند.

۲- نسبت به استفاده از روشهایی که موجب بالا بردن امنیت در استانداردهای وب همچون WSDL UDDI و SOAPمی شود، توجه کافی داشته باشند. همچنین علاوه بر کنترل دسترسی با استفاده از فهرست راهنما، روشهای دیگر کنترل دسترسی را مد نظر قرار دهند.

منابع

ایزدی، م، ۱۳۸۹، امنیت در سیستم های اطلاعاتی توسعه یافته با روش معماری سرویسگرا. پایان نامه کارشناسی ارشد رشته مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه علامه طباطبایی.

تاجیک، محمدرضا،۱۳۷۷، قدرت و امنیت در عصر پسامدرنیسم گفتمان، شماره صفر.

جلالی فراهانی، امیرحسین، ۱۳۸۵،پیشگیری وضعی از جرایم سا یبر در پرتو مواز ین حقوق بشر فصلنامۀ فقه و حقوق، قم، سال دوم،ص۱۴-۱۸.

دارا، ع. ۱۳۸۸، معماری سرویسگرا با بررسی دیدگاههای امنیتی آن، سمینار کارشناسی ارشد. دانشگاه آزاد اسلامی واحد علوم و تحقیقات.

رابرت، ماندل،۱۳۷۷، چهره متغیر امنیت ملی تهران:پژوهشکده مطالعات راهبردی.

رنجبر، مقصود،۱۳۷۹، ملاحظات امنیتی در سیاست خارجی جمهوری اسلامی ایران تهران:پژوهشکده مطالعات راهبردی

سجادی، سیدحسین؛ طباطبایی نژاد، سید محسن،سیستم های اطلاعات حسابداری، انتشارات دانشگاه شهید چمران، چاپ اول.

صفار، محمد جواد،۱۳۸۵، بیانیه شش شبکه جهانی حسابرسی"، حسابرس، شماره ۳۵.

عبداللهی ازگمی، محمد؛۱۳۷۵، طراحی و پیاده سازی سرویس های امن برای شبکه های رایانه ای پایان نامۀ کارشناسی ارشد ، تهران:دانشگاه صنعتی شریف.

مولانا، حمید. ،۱۳۷۹،جریان بین المللی اطلاعات ،ترجمۀ یونس شکرخواه. تهران:مرکز مطالعات و تحقیقات رسانه ها.

میرمجبیان، حمید، شهشهانی، سید محمد حسن،۱۳۸۵، کارایی تصمیم گیری در گزارشگری مالی در محیط شبکه گسترده جهانی"، حسابرس، شماره ۳۵.

ودیعی، محمد حسین، موسوی نژاد، سید روحا. ،۱۳۸۷،حسابرسی در عصرتجارت الکترونیک"، حسابرس، شماره۴۱.

Afshar, M. , Kavantzas, N. , Turlapati, R. (2006). Best Practices for Securing Your SOA:A Holistic Approach. *Java Developers Journal*, 8(2):11-23.

Brose, G. (2003). *Service Web Services with SOAP Security Proxies*. Proceeding of the 13th International Conference, 7-9 September, Dresden, Germany.

Buecker, A. , Ashley, P. & Borrett, M. , Readshaw, N. (2007). Understanding SOA Security Design and Implementation. *International Technical Support Organization*, Brussels, IBM redbook Publication Candolin, C. (2007). A Security Framework for Service Oriented Architectures. Proceeding of the 5th Military Communications Conference,15-17 October, Florida.

Casola,V. (2007). A Policy-Based Evaluation for Quality and Security in Service Oriented Architectures. 6th IEEE International Conference Web Services, 3-5 May, Leipzig, Germany.

Chodavarapu, P. and Kanneganti, R. (2007). SOA Security. 8th International Conference Web Services, 10-12 December, Grenoble, France.

Fareghzadeh, N. (2009). Web Service Security Method To SOA Development. *World Academy of Science Engineering and Technology*, 49(5):36-48.

Siming, K. & Babar, M. (2010). *Modeling Security for Service Oriented Applications*. Proceeding of The 8th European Conference on Software Architecture, 13-15 May, Nottingham.

Weilye, K. & Wing, J. (2005). Game Strategies in Network Security. *International Journal of Information Security*, 4(2):17-28.
Yamany, H. , Miriam, C. (2010). Intelligent Security and Access Control Framework for Secure-Oriented architecture. *Information and Software Technology*, 25 (2):220-236.
Yamany, H. & Tao, X. (2012). *Web Services Security Problem Insecure-oriented Architecture*. International Conference on Applied Physics and Industrial Engineering, 24(6):1635-1641.