DOI: http://dx.doi.org/10.22059/jitm.2013.36502

مدیریت فناوری اطلاعات
دانشکده مدیریت دانشگاه تهران
دوره ۵، شماره ۳
پاییز ۱۳۹۲
صص ۴۲-۲۵

بررسی امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با روش معماری سرویس‌گرا(SOA)

محمدرضا تقوا[۱]، ماندانا ایزدی[۲]

چکیده: مزایا و ویژگی‌های خاص معماری سرویس‌گرا و گسترش به‌کارگیری این معماری، درعمل مباحث امنیتی مرتبط با SOA را که در پاره‌ای 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 IT در برقراری یک سیستم اطلاعاتی ایمن و ایمن‌سازی هر چه بهتر معماری سرویس‌گرا یاری رساند. پژوهش حاضر از دید هدف کاربردی و از دیدگاه روش انجام پژوهش، توصیفی شمرده می‌شود. در این مطالعه بعد از استخراج مهم‌ترین شاخص‌ها، از نمونه آماری در این باره پرسش به‌عمل آمد. پس از گردآوری داده‌ها با کمک آزمون تی، به تجزیه و تحلیل آنها پرداخته شد. سپس با کمک تحلیل سلسله‌مراتبی داده‌ها، مهم‌ترین ابعاد امنیتی و زیر ابعاد مربوط به هریک، به‌ترتیب اهمیت اولویت‌بندی شدند.

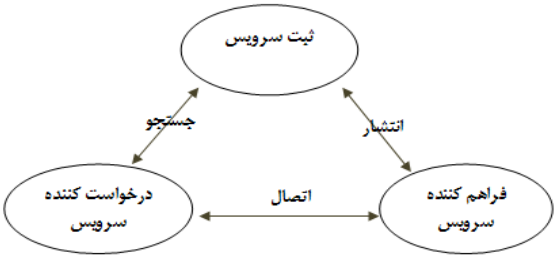
واژه‌های کلیدی: امنیت وب سرویس، سرویس، معماری سرویس‌گرا.

۱. استادیار دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبایی، تهران، ایران
۲. کارشناس ارشد رشته مدیریت فناوری اطلاعات، دانشگاه علامه طباطبایی، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۱/۰۸/۲۰
تاریخ پذیرش نهایی مقاله: ۹۲/۰۵/۱۶
نویسنده مسئول مقاله: ماندانا ایزدی
E-mail: m_izadi85@yahoo.com

مقدمه

معماری سرویس‌گرا که امروزه اکثر سازمان‌ها در سراسر جهان آن را پذیرفته‌اند، توانسته است افزون‌بر حل برخی مشکلات، مزایای زیادی را برای سازمان‌ها به‌همراه داشته باشد؛ اما علاوه‌بر مزایای بی‌شماری که این معماری به‌همراه دارد، ویژگی‌های خاص معماری سرویس‌گرا، از جمله باز بودن مرزهای آن، موجب شده تا امنیت این سیستم اطلاعاتی در مقایسه با سایر سیستم‌های اطلاعاتی بیشتر در معرض خطر قرار گیرد. به‌همین دلیل محافظت از این نوع سیستم‌های اطلاعاتی که یک نوع دارایی سازمان به‌شمار می‌روند، اهمیت بسیاری پیدا می‌کند (ایزدی، ۱۳۸۹). در همین ارتباط، هدف این پژوهش بررسی ابعاد مختلف امنیتی و ارائه راهکارهایی برای برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا است. معماری سرویس‌گرا دارای ساختار توزیع شده‌ای است و تأکید آن بر تجزیه عملیات کسب‌وکاری پیچیده به اجزایی است که قابل استفاده مجدد باشد و مزایای بیشتری را از استانداردسازی فرآیندهای کسب‌وکاری ارائه دهد که این اجزا، همان سرویس‌ها هستند. به‌گفته‌ای، سرویس‌ها اجزای توزیع شده با رابطه‌ای تعریف شده هستند که پیام‌های XML را پردازش و تبادل می‌کنند. یکپارچگی و تعامل بین سرویس‌ها از طریق فناوری وب سرویس و از طریق استانداردهایی مانند WSDL، SOAP، UDDI انجام می‌شود (Hammar, 2006). مدل پایه SOA از سه جزء اصلی درخواست‌کننده سرویس، فراهم‌کننده سرویس و کشف سرویس تشکیل شده است که ارتباط این سه عامل شامل منتشر کردن، پیدا کردن و متصل شدن به سرویس است. فراهم‌کننده سرویس پیاده‌سازی، از طریق شبکه به ارائه توضیحات آن سرویس برای عامل کشف سرویس می‌پردازد. درخواست کننده معمولا درخواست پیدا کردن سرویس را به عامل کشف سرویس می‌دهد تا از طریق آن به توضیحات ارائه شده سرویس و محل آن دسترسی پیدا کند. سپس با به‌کارگیری این اطلاعات به فراهم‌کننده سرویس، متصل شده و از سرویس ارائه شده استفاده می‌کند (Chodavarapu & Kanneganti, 2007).



نمودار ۱. مدل پایه معماری سرویس‌گرا (Chodavarapu & Kanneganti, 2007)

در واقع این معماری به‌دلیل ماهیت توزیع‌پذیری، تعامل‌پذیری ذاتی، قابلیت استفاده مجدد، دسترسی باز و ویژگی‌های دیگر، دارای جنبه‌ها و نیازمندی‌های جدید و بیشتری نسبت به روش‌های قبلی است، بنابراین مدل امنیتی SOA باید به‌گونه‌ای باشد که ضمن حفظ امنیت، موجب شود تا چابکی، انعطاف‌پذیری، استفاده بهتر از سرویس‌ها و امکانات درون‌سازمانی و بین سازمانی فراهم شود (Hafner, 2009).

یکی از مسائل دیگری که در امنیت SOA باید مورد توجه قرار گیرد، باز نگه‌داشتن سرویس‌ها و قابلیت تعامل بین آنها است. از آنجا که استفاده از وب سرویس، گسترده‌ترین نگرش پذیرفته‌شده در به‌کارگیری SOA است، به‌همین دلیل بیشتر جنبه‌های امنیتی در این نوع معماری بر امنیت وب سرویس‌ها متمرکز است (Fareghzadeh, 2009).

مهم‌ترین جنبه‌های امنیتی که باید در معماری سرویس‌گرا به آن توجه شود، شامل: در نظر گرفتن یک سیاست امنیتی جامع، در نظر گرفتن امنیت به‌منزله یک سرویس و مورد توجه قرار دادن عواملی همچون احراز هویت، کنترل دست‌یابی، تمامیت و محرمانگی پیام، امنیت سطح پیام، امنیت در سطح نقل و انتقال، در دسترس بودن یک سرویس یا یک درخواست، ممیزی به‌معنای بررسی و حسابرسی داده‌ها، فرآیندها، تراکنش‌های انجام شده در سیستم‌های اطلاعاتی، مدیریت‌کردن امنیت، مدیریت‌کردن سیاست، مدیریت سیاست امنیتی، نظارت و مدیریت ریسک و عوامل دیگری چون امنیت منابع انسانی، امنیت محیط و امنیت منابع فیزیکی و مانند آن می‌شود (Siming & Babar, 2010; Xiaoming, 2006). در این پژوهش، برای بررسی و استخراج ابعاد مختلف امنیتی و ارائه راهکارهایی برای امنیت این نوع معماری، نخست ادبیات پژوهش مربوط به آن مورد مطالعه قرار گرفت و پس از مصاحبه با خبرگان و استخراج شاخص‌های نهایی، به تهیه پرسش‌نامه، جمع‌آوری و تجزیه و تحلیل داده‌ها پرداخته شد و نتیجه نهایی ارائه شد.

بیان مسئله

مزایای رقابتی معماری سرویس‌گرا سبب رشد روزافزون این معماری، به‌ویژه در دو دهه اخیر در سراسر جهان شده است؛ اما ویژگی خاص معماری سرویس‌گرا، از جمله خاصیت توزیع‌شدگی و باز بودن مرزهای آن موجب شده تا امنیت این معماری با چالش‌هایی همچون نبودن مفهوم پیوستگی، احراز هویت برای سرویس‌های بیرونی، امنیت بین مرزها، امنیت برنامه‌های کاربردی که از ترکیب چندین سرویس تشکیل شده‌اند و ... همراه باشد. گرچه هر ساله تعداد مقاله‌هایی که به جنبه خاصی از امنیت معماری سرویس‌گرا می‌پردازند، در حال افزایش است؛ اما به نظرمی‌رسد به‌دلیل نو پا بودن این نوع معماری و عدم شناخت بسیاری از خبرگان حوزه سیستم‌های

اطلاعاتی و شبکه و چالش‌های موجود در زمینه امنیت معماری سرویس‌گرا، هنوز کتاب‌ها و مقاله‌های چندانی در این زمینه تألیف نشده است. هدف این پژوهش کمک به تصمیم‌گیری بهتر مدیران و مجریانی است که مسئول برقراری امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا هستند. این پژوهش در قالب هفت فرضیه اصلی و سی‌وسه فرضیه فرعی است که فرضیه‌های اصلی به شرح زیر هستند:

فرضیه۱: امنیت در قسمت طراحی و پیاده‌سازی معماری، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه۲: امنیت شبکه و وب سرویس، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه۳: امنیت داده، می‌تواند به‌منزله یکی از شاخص‌های مؤثر دربرقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه۴: امنیت در قسمت مدیریت، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه۵: امنیت در قسمت منابع فیزیکی و محیط، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه۶: امنیت در قسمت منابع انسانی، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

فرضیه۷: امنیت در قسمت برنامه‌های کاربردی، می‌تواند به‌منزله یکی از شاخص‌های مؤثر در برقراری امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا شمرده شود.

ادبیات نظری پژوهش

معماری سرویس‌گرا، روشی برای ساخت سیستم‌های توزیع شده‌ای است که در آنها عملکرد سیستم، به‌صورت سرویس در اختیار کاربران یا سایر سرویس‌ها قرار می‌گیرد. این نوع معماری به‌دلیل مزایای بی‌شمار خود، امروزه از سوی اکثر سازمان‌ها 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 سیستم‌های اطلاعاتی بیشتر در معرض خطر قرار گیرد. در حال حاضر یکی از مشکلات بزرگ در گسترش این معماری، چالش‌های امنیتی موجود در آن است. از دسته مهم‌ترین جنبه‌های امنیتی معماری سرویس‌گرا مواردی است که در زیر اشاره شده است:

سیاست امنیتی: یک سیاست امنیتی، اهداف، محدوده امنیت اطلاعات مطلوب، اهمیت امنیت به‌منزله یک عامل مهم برای توسعه سازمان، پشتیبانی به‌منظور معرفی سیستم‌های امنیتی، اصول اولیه به‌کارگیری امنیت اطلاعات، مسئولیت که مرتبط هستند به معرفی این سیستم‌ها، اسناد و آیین‌نامه‌هایی برای کارمندان در رابطه با سیستم‌های امنیتی را تعریف می‌کند (Ashley, Buecker, 2007).

امنیت به‌منزله یک سرویس: به‌طور کلی در مدل امنیت به‌منزله یک سرویس، منطق امنیت به‌صورت بخشی از یک کاربرد یا بخشی از منطق یک سرویس نیست، بلکه به‌صورت مجزا و متمرکز در یک سرویس امنیتی پیاده‌سازی می‌شود. تمامی تبادلات به‌صورت داده، پیام، درخواست و... نخست تحت کنترل و نظارت این سرویس قرار می‌گیرد (دارا، ۱۳۸۸).

احراز هویت: احراز هویت در شبکه‌های رایانه‌ای، بدین معناست که یک سرویس‌دهنده بتواند تشخیص دهد فرد یا سرویسی که تقاضایی را روی آن سیستم دارد، مجاز است یا نه؟ (دارا، ۱۳۸۸).

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

تمامیت و محرمانگی پیام: تمامیت پیام، تضمین می‌کند پیام یا داده‌های دریافتی، به‌طور دقیق همان چیزی است که از جانب نهاد مجاز ارسال شده است و فاقد هرگونه تغییر، درج، حذف یا تکرار است.

محرمانگی را می‌توان به‌معنای حفاظت اطلاعات از افشاگری غیر مجاز دانست. به‌گفته‌ای اطلاعات فقط باید برای افراد مجاز در دسترس باشد که معمولاً در دو سطح پیام و نقل و انتقالات به‌کار برده می‌شود (دارا، ۱۳۸۸).

در دسترس بودن: در دسترس بودن یک سرویس یا درخواست، نشان‌دهنده این است که آن سرویس قادر است پاسخ به یک سرویس را به‌موقع فراهم کند و اطمینان می‌دهد که سرویس‌ها، زمانی که درخواست در بسیاری از محیط‌های SOA کلیدی است، در دسترس هستند (دارا، ۱۳۸۸).

امنیت در سطح پیام: برای امنیت در سطح پیام، می‌توان از مسیریابی پیام‌ها استفاده کرد؛ یعنی پیام‌ها به‌سمت نقاط انتهایی معتبری که مد نظر است، هدایت می‌شوند. برای مثال، پیام

درصورتی به سمت سرویس A هدایت می‌شود که درخواست‌کننده، ویژگی‌های X و Y را داشته باشد. یک دیدگاه دیگر اینست که بخش‌های مختلف یک پیام، می‌توانند به‌طور مجزا محافظت شوند تا در مسیر پیام، تنها توسط بخش‌هایی که مورد نظر است، قابل استفاده باشد (دارا، ۱۳۸۸).

امنیت در سطح نقل و انتقالات: برای امنیت در سطح نقل و انتقالات از SSL/TLS برای مخفی کردن شبکه‌های ارتباطی از اده مشتریان سرویس استفمی‌شود. کاربردها به کمک SSL/TLS کانال‌های ایمنی را برای تبادل داده‌ها برقرار می‌کنند (دارا، ۱۳۸۸).

ممیزی: ممیزی به معنای بررسی و حسابرسی داده‌ها، فرآیندها، تراکنش‌های انجام شده در سیستم‌های اطلاعاتی است که به منظور برآورده شدن ملزومات امنیتی انجام می‌گیرد (Ashley & Buecker, 2007).

مدیریت امنیت: مدیریت امنیت، مدیریت تمامی مراحل و راهکارهای امنیتی از ایجاد و تأمین امنیت، محافظت و نگهداری، کنترل و بازرسی امنیت و... را شامل می‌شود (دارا، ۱۳۸۸).

مدیریت سیاست: اهدافی که به‌وسیله کسب‌وکار ایجاد شده و به حرکت درآمده‌اند، اکنون باید به‌وسیله زیرساختارها اجرا شوند. مدیریت سیاست یک چارچوبی را برای اجرا کردن سیاست فراهم می‌کند (Ashley & Buecker, 2007).

مدیریت سیاست امنیتی: مدیریت سیاست‌های امنیتی با معرفی سیاست‌های کسب‌وکاری و با معرفی سیاست‌های خاص سرویس، مانند امنیت، شاخص‌های عملکرد، سیاست‌های مطمئن و... آغاز می‌شود. این سیاست‌ها به‌وسیله زیرساخت‌ها برای امنیت دسترسی به اطلاعات، فراهم‌کردن دسترسی، نگهداری، توانایی ممیزی و مانند آنها اداره می‌شود (Ashley & Buecker, 2007).

ادبیات تجربی پژوهش

در زمینه امنیت اطلاعات در معماری سرویس‌گرا، پژوهش‌های متعددی انجام شده است، از آن دسته می‌توان به دسترسی چارچوب کنترل امنیت هوشمند و معماری سرویس‌گرا (Yamany & Miriam, 2010)، مشکلات سرویس‌دهی وب در طراحی معماری سرویس‌گرا (Yue & Tao, 2012)، معماری سرویس‌گرا برای امنیت سیستم شبکه همراه (Rosado & Eduardo, 2011)، امنیت و کاربرد آن در برنامه‌های معماری سرویس‌گرا (Hangjung & Nazareth, 2010) اشاره کرد؛ اما اکثر این مطالعات با یک رویکرد فنی و هر کدام تنها به یک جنبه خاص امنیت این معماری پرداخته‌اند و کمابیش هیچکدام با یک دید کلی و یک رویکرد سیستمی به بررسی این موضوع نپرداخته‌اند.

الیمنی و همکاران (۲۰۱۰) در پژوهشی با عنوان «دسترسی چارچوب کنترل امنیت هوشمند و معماری سرویس‌گرا»، بیان کردند یکی از مشکلات بزرگ گسترش معماری سیستم‌گرا چالش‌های امنیتی موجود در آن است؛ چراکه مسئولیت امنیت SOA به هر دو گروه ارائه‌دهندگان و مصرف‌کنندگان، وابسته است. آنان معتقدند در سال‌های اخیر، تلاش‌های زیادی برای رفع این نواقص انجام شده است که از آن دسته، دسترسی به استانداردهای امنیتی شبکه وب که شامل WS-Security و WS-Policy، بوده است. در این پژوهش یک چارچوب هوشمند امنیتی پیشنهاد شده است که شامل دو عامل مهم در زمینه دست‌یابی به امنیت است: ۱. احراز هویت و امنیت خدمات (NSS) و ۲. سرویس مختار (AS). در این پژوهش از سه نوع مختلف داده‌کاوی استفاده شده است: ۱. قوانین انجمن که به پیش‌بینی حمله‌ها کمک می‌کند؛ ۲. مکعب پردازش تحلیلی برخط برای مجوز استفاده و ۳. الگوریتم کاوش استخراجی که دسترسی به کنترل نمایندگی حقوق و سیستم خودکار را فراهم می‌کند (Yamany & Miriam, 2010).

یو و تائو (۲۰۱۲) در پژوهشی با عنوان «مشکلات سرویس‌دهی وب در طراحی معماری سرویس‌گرا» بیان کرده‌اند که با توسعه جهانی استفاده از فناوری SOA، مسائل امنیتی خدمات تارنما (وب‌سایت) که بر اساس پلت‌فرم ناهمگون شکل گرفته‌اند، به‌طور فزاینده‌ای برجسته و مهم خواهد شد. در این پژوهش دو راهکار امنیتی برای خدمات سرویس‌دهی ارائه شده است (Yue & Tao, 2012).

روسادو و همکاران (۲۰۱۱) در مطالعه‌ای با موضوع معماری سرویس‌گرا برای امنیت سیستم شبکه همراه بیان کردند که امنیت در سیستم‌های شبکه همراه، بسیار ضروری است؛ در حالی‌که تأمین امنیت این سیستم‌ها به‌دلیل کمبود منابع در این دستگاه‌ها، سخت و پیچیده است. در این پژوهش برای حفظ امنیت این سیستم‌ها، از مدلی بر اساس طراحی معماری سرویس‌گرا استفاده شده است. این مدل تا اندازه‌ای محدودیت‌های دسترسی به امنیت شبکه‌های تلفن همراه را برآورده می‌کند؛ اما نتایج پژوهش نشان می‌دهد که این مدل به‌طور کامل راهگشا نبوده است (Rosado & Eduardo, 2011).

زو و همکاران در سال ۲۰۱۰ در پژوهشی با عنوان «امنیت و کاربرد در برنامه‌های معماری سرویس‌گرا؛ موضوعات تجارتی»، معتقدند با پیشرفت کاربرد محاسبات و طراحی معماری سرویس‌گرا و گسترش استفاده از این خدمات، از برنامه‌های کاربردی زیادی با توسعه مؤلفه‌های نرم‌افزاری و شبکه‌های استاندارد، استفاده خواهد شد. این برنامه‌ها به لحاظ هزینه و پتانسیل تولید نسبی بالاتر، به‌وسیله طراحی معماری سرویس‌گرا تعدیل خواهند شد و تنها مشکل موجود، تأمین امنیت کاربری این برنامه‌ها و شبکه‌ها است. در این پژوهش از یک الگوریتم ژنتیک برای

یافتن مجموعه‌ای بهینه از خدماتی که از پروسه‌های تجاری این خدمات پشتیبانی کند، استفاده شده است. آنها معتقدند که کاربرد این روش در آینده گسترده‌تر خواهد شد (Hangjung & Nazareth, 2010).

روش پژوهش

این پژوهش از دید هدف کاربردی و از نظر روش‌شناسی، توصیفی شمرده می‌شود. این پژوهش در چارچوب هفت فرضیه اصلی و سی‌وسه فرضیه فرعی، به بررسی ابعاد مختلف امنیتی و زیرابعاد مربوط به آنها پرداخته است. بُعد امنیتی اول (امنیت در پیاده‌سازی و طراحی معماری سرویس)، بُعد امنیتی دوم (امنیت سطح شبکه و وب)، بُعد امنیتی سوم (امنیت در سطح داده)، بُعد امنیتی چهارم (امنیت در بخش مدیریت سیستم اطلاعاتی)، بُعد امنیتی پنجم (امنیت در بخش منابع فیزیکی و محیط)، بُعد امنیتی ششم (امنیت منابع انسانی)، بُعد امنیتی هفتم (امنیت برنامه‌های کاربردی) است. هر یک از این ابعاد امنیتی نیز خود دارای زیر ابعادی هستند.

جدول ۱. نتایج پایایی هر یک از ابعاد امنیتی

فرضیه‌ها	تعداد سؤال‌های مربوط به هر فرضیه	محاسبه آلفای کرونباخ برای هر بُعد امنیتی
فرضیه۱ـ بُعد امنیتی اول (امنیت در پیاده سازی و طراحی معماری سرویس‌گرا) (Heather, 2005)	۲	۰/۷۱۲
فرضیه۲ ـ بُعد امنیتی دوم (امنیت سطح شبکه ووب) (Ashley & Buecker, 2007)	۷	۰/۷۳۲
فرضیه۳ ـ بُعد امنیتی سوم(امنیت داده) (Jonnaganti,2009)	۸	۰/۷۶۶
فرضیه۴ ـ بُعد امنیتی چهارم (امنیت در قسمت مدیریت) (دارا، ۱۳۸۸)	۳	۰/۸۱۲
فرضیه۵ ـ بُعد امنیتی پنجم (امنیت منابع فیزیکی) (Ashley & Buecker, 2007)	۲	۰/۸۲۱
فرضیه۶ ـ بُعد امنیتی ششم (امنیت منابع انسانی)(Jonnaganti,2009)	۳	۰/۸۱۲
فرضیه۷ ـ بُعد امنیتی هفتم (امنیت منابع کاربردی) (Ashley & Buecker, 2007)	۸	۰/۷۴۲

روش محاسبه جامعه آماری و نمونه‌گیری

جامعه آماری در نظر گرفته شده در این پژوهش، شامل تمامی خبرگانی می‌شود که در سطح شهر تهران در زمینه امنیت سیستم‌های اطلاعاتی که بر پایه معماری سرویس‌گرا پایه‌ریزی شده، مشغول فعالیت بوده یا دست‌کم سه سال سابقه کار در زمینه امنیت سیستم‌های اطلاعاتی و امنیت شبکه را داشته و از دانش کافی در مورد معماری سرویس‌گرا برخوردار باشند. از آنجا که تعداد افرادی که در این زمینه مشغول فعالیت هستند، بسیار محدود و پراکنده است و اندازه دقیق جامعه آماری در دسترس نبود، بر اساس بررسی انجام گرفته و شناسایی خبرگان و کارشناسان این حوزه، نمونه‌گیری به‌صورت قضاوتی انجام گرفت و از حدود ۴۷ پرسش‌نامه توزیع شده، ۴۰ پرسش‌نامه دریافت شد که مشخصات پاسخ‌دهندگان در جدول شماره ۱ آورده شده است.

جدول ۲. مشخصات خبرگان

ردیف	سمت	نوع تخصص	تعداد	تحصیلات	تجربه
۱	مدیر فناوری اطلاعات	امنیت اطلاعات و شبکه، فناوری اطلاعات	۳	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۲	مدیر امنیت شبکه و اطلاعات	امنیت اطلاعات و شبکه، فناوری اطلاعات	۱۲	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۳	کارشناس ارشد امنیت شبکه	امنیت اطلاعات و شبکه، فناوری اطلاعات	۴	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۴	کارشناس سیستم مدیریت امنیت اطلاعات	امنیت اطلاعات و شبکه، فناوری اطلاعات	۶	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۵	کارشناس امنیت شبکه و نرم‌افزار	امنیت اطلاعات و شبکه، فناوری اطلاعات	۱۴	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا
۶	کارشناس ارتباطات شبکه	امنیت اطلاعات و شبکه، فناوری اطلاعات	۱	کارشناس و کارشناس ارشد (سخت‌افزار، نرم‌افزار، مهندسی فناوری اطلاعات)	۳ سال به بالا

ابزار و روش گردآوری داده‌ها

روش گردآوری اطلاعات نیز با استفاده از دو شیوه کتابخانه‌ای و استفاده از پرسش‌نامه انجام گرفته است. روایی پژوهش از طریق مطالعه مبانی نظری و با استفاده از نظر استادان و متخصصان در این زمینه لحاظ شد و پایایی ابزار پژوهش از طریق آزمون ضریب آلفای کرونباخ محاسبه شد که مقدار آن برابر با ۰/۹۳۵ به‌دست آمد. برای پاسخ‌دهی به سؤال‌های پژوهش و تحلیل داده‌ها از روش‌های آماری استفاده شد. با توجه به اینکه جامعه پژوهش حاضر نرمال و تعداد نمونه آن بیش از ۳۰ نفر بود، داده‌های جمع‌آوری شده از طریق پرسش‌نامه به‌صورت استنباطی و با استفاده از آزمون تی ـ استیودنت مورد تجزیه و تحلیل قرار گرفت. با توجه به اینکه

در پرسش‌نامه از مقیاس لیکرت پنج‌گزینه‌ای استفاده شده است و میانگین این مقیاس ۳ محاسبه شد، بنابراین میانگین جامعه مورد نظر در تحلیل‌ها نیز رقم ۳ در نظر گرفته شده است و آزمون‌های فرض آماری نیز به‌صورت رابطه شماره ۱و ۲ در نظر گرفته شده است که ادعای ما در فرض H_1 قرار می‌گیرد

رابطه ۱) $H_{0:}\ \mu \leq 3$

رابطه ۲) $H_1 :\mu \geq 3$

سپس برای وزن‌دهی و اولویت‌بندی کردن مهم‌ترین شاخص‌ها و زیر شاخص‌های مربوط به آنها، با استفاده از روش‌های تصمیم‌گیری چند متغیره برای اولویت‌بندی کردن بر اساس اهمیت و وزن‌دهی به هریک از شاخص‌ها استفاده شده است.

یافته‌های پژوهش

نتایج و یافته‌های حاصل از تجزیه و تحلیل فرضیه‌ها با کمک آزمون t در سطح ۰/۰۵ =α به شرح زیر است:

جدول۳. نتایج تجزیه و تحلیل داده‌های مربوط به ابعاد امنیتی و زیرشاخص‌های آنها

شاخص‌های اصلی	مقدارآماره آزمون تی.	نتیجه‌گیری
فرضیه۱	۶/۴۸۹	رد فرض صفر
فرضیه۲	۱۲/۹۳۰	رد فرض صفر
فرضیه۳	۱۴/۴۱۶	رد فرض صفر
فرضیه۴	۱۲/۳۲۴	رد فرض صفر
زیرشاخص‌های امنیت داده	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
محرمانگی (Jonnaganti, 2009)	۱۸/۰۲۸	رد فرض صفر
جامعیت (Jonnaganti, 2009)	۷/۷۰۶	رد فرض صفر
دسترس پذیری (Jonnaganti, 2009)	۸/۴۷۳	رد فرض صفر
احراز هویت (Jonnaganti, 2009)	۶/۶۸۴	رد فرض صفر
شاخص‌های اصلی	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
فرضیه۵	۷/۸۲۹	رد فرض صفر
فرضیه۶	۱۲/۷۴۵	رد فرض صفر
فرضیه۷	۱۴/۴۹۳	رد فرض صفر
زیرشاخص‌های معماری	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
امنیت به‌منزله یک سرویس (Heather, 2005)	۶/۴۰۷	رد فرض صفر
(Heather, 2005) ESB & gateway	۵/۴۵۴	رد فرض صفر

ادامه جدول ۳. نتایج تجزیه و تحلیل داده‌های مربوط به ابعاد امنیتی و زیرشاخص‌های آنها

زیرشاخص‌های بخش مدیریت	مقدارآماره آزمون تی.	نتیجه‌گیری
مدیریت سیاست امنیتی (دارا، ۱۳۸۸)	۱۷/۷۱۶	رد فرض صفر
مدیریت ریسک (دارا، ۱۳۸۸)	۱۹/۰۷۱	رد فرض صفر
مدیریت سیاست (دارا، ۱۳۸۸)	۱۷/۷۱۶	رد فرض صفر
زیرشاخص‌های امنیت داده	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
تعیین سطح دسترسی (Heather, 2005)	۴/۵۵۵	رد فرض صفر
تشخیص و شناسایی (Heather, 2005)	۸/۵۴۰	رد فرض صفر
امنیت نقل و انتقال (Heather, 2005)	۱۰/۹۸۱	رد فرض صفر
سیاست امنیتی (Heather, 2005)	۱۲/۴۹۰	رد فرض صفر
زیرشاخص‌های منابع فیزیکی	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
تجهیزات (Ashley & Buecker, 2007)	۹/۹۵۱	رد فرض صفر
بازبینی‌های عمومی (Ashley & Buecker, 2007)	۵/۵۳۰	رد فرض صفر
زیرشاخص‌های منابع انسانی	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
تحصیل (Jonnaganti, 2009)	۱۷/۷۱۶	رد فرض صفر
آموزش (Jonnaganti, 2009)	۵/۷۳۰	رد فرض صفر
آگاهی (Jonnaganti, 2009)	۱۷/۷۱۶	رد فرض صفر
زیرشاخص‌های برنامه‌های کاربردی	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
محرمانگی(Jonnaganti, 2009)	۱۹/۰۷۱	رد فرض صفر
جامعیت (Jonnaganti, 2009)	۵/۴۱۴	رد فرض صفر
دسترس پذیری (Jonnaganti, 2009)	۹/۸۰۲	رد فرض صفر
احراز هویت (Jonnaganti, 2009)	۱۰/۳۵۶	رد فرض صفر
تشخیص و شناسایی (Jonnaganti, 2009)	۲/۹۳۳	رد فرض صفر
ممیزی و نظارت (Jonnaganti, 2009)	۹/۰۶۷	رد فرض صفر
سیاست امنیتی (Jonnaganti, 2009)	۱۷/۷۱۶	رد فرض صفر
تعیین سطح اختیار (Jonnaganti, 2009)	۸/۲۰۴	رد فرض صفر
زیرشاخص‌های شبکه	**مقدارآماره آزمون تی.**	**نتیجه‌گیری**
ایزولاسیون (Ashley & Buecker, 2007)	۲/۹۳۳	رد فرض صفر
کنترل ترافیک (Ashley & Buecker, 2007)	۸/۴۷۳	رد فرض صفر
امنیت IP (Ashley & Buecker, 2007)	۱۰/۳۵۶	رد فرض صفر
محکم کردن پایه‌های امنیتی اجزا (Jonnaganti,2009)	۵/۴۵۴	رد فرض صفر
مدیریت رویدادها (Ashley & Buecker, 2007)	۰/۶۴۹	تایید فرض صفر
حفاظت در مقابل حمله‌ها(Jonnaganti,2009)	۱۰/۸۹۱	رد فرض صفر
کشف و جلوگیری از تجاوز (Jonnaganti,2009)	۱۰/۳۵۶	رد فرض صفر
امنیت نقل و انتقال (Jonnaganti,2009)	۵/۸۴۹	رد فرض صفر

جدول ٤. نتایج تجزیه و تحلیل راهکارهای امنیتی

راهکارهای امنیت شبکه	مقدارآماره آزمون تی.	نتیجه‌گیری
استفاده از فایروال	۹/۸۷۴	رد فرض صفر
ارزیابی آسیب‌ها	۸/۸۶۸	رد فرض صفر
سیاست‌های امنیتی	۱۳/۸۰	رد فرض صفر
پروکسی	۸/۸۶۸	رد فرض صفر
راهکارهای امنیت پیام	**مقدار آماره آزمون تی.**	**نتیجه‌گیری**
WS-security	۸/۸۴۷	رد فرض صفر
مسیریابی پیام‌ها	۱۰/۲۳۲	رد فرض صفر
حفاظت از بخش‌های مختلف پیام	۱۱/۷۷۷	رد فرض صفر
راهکارهای امنیت منابع انسانی	**مقدار آماره آزمون تی.**	**نتیجه‌گیری**
تحصیل	۷/۳۴۱	رد فرض صفر
آموزش	۵/۲۷۹	رد فرض صفر
آگاهی	۲۰/۱۵۶	رد فرض صفر
راهکارهای سیاست‌های امنیتی	**مقدار آماره آزمون تی.**	**نتیجه‌گیری**
WS-security policy	۱۷/۸۳	رد فرض صفر
استفاده از تجرید یا انتزاع در طراحی سیاست‌ها	۵/۱۱۱	رد فرض صفر
راهکارهای سطح دسترسی	**مقدار آماره آزمون تی.**	**نتیجه‌گیری**
دسته‌بندی کاربرد، دیتابیس	۹/۰۹۸	رد فرض صفر
تکثیر سرویس‌ها	۳/۳۲۳	رد فرض صفر
راهکارهای احراز هویت	**مقدار آماره آزمون تی.**	**نتیجه‌گیری**
استفاده از شناسه کاربری	۷/۰۵۴	رد فرض صفر
رمزنگاری با کلید عمومی و خصوصی	۷/۲۷۴	رد فرض صفر
سرویس‌دهنده راهنما	۴/۵۲۶	رد فرض صفر
توکن‌های امنیتی	۱۴/۸۶۴	رد فرض صفر
راهکارهای نقل و انتقال	**مقدار آماره آزمون تی.**	**نتیجه‌گیری**
Ws-reliable messaging	۶/۸۲۹	رد فرض صفر
S-HTTP , SSL/TLS	۶/۵۲۵	رد فرض صفر

برای تعیین میزان اهمیت و تأثیری که هریک از این ابعاد و زیر ابعاد مربوط به آنها در برقراری امنیت در سیستم‌های اطلاعاتی سرویس‌گرا دارند، از نظر خبرگان مقایسات زوجی انجام گرفت و با کمک نرم‌افزار expert choice اوزان مربوط به هریک محاسبه شد. سپس با کمک تحلیل سلسله‌مراتبی داده‌ها، هر یک از ابعاد و زیر ابعاد مربوط به آن، بر اساس اهمیت به‌ترتیب زیر اولویت‌بندی شدند.

جدول ۵. اولویت‌بندی ابعاد امنیتی و زیر ابعاد مرتبط با آنها با کمک روش AHP

ردیف	۱	۲	۳	٤	٥	٦	۷
معیارهای اصلی SOA	امنیت داده	امنیت شبکه و وب	امنیت در مدیریت	منابع فیزیکی	امنیت در منابع انسانی	امنیت معماری	برنامه‌های کاربردی
وزن نهایی	۰/۳۲۰	۰/۱۲۰	۰/۱۶۶	۰/۰۶۸	۰/۰۵۸	۰/۲۳۷	۰/۰۹۷
اولویت	۱	۵	۳	۶	۷	۸	۴

زیرشاخص‌های امنیت شبکه و وب	ایزولاسیون	کنترل ترافیک بین شبکه	محکم کردن پایه‌های امنیتی اجزا	امنیتIP	کشف و جلوگیری از تجاوز	حفاظت در مقابل حمله‌ها	امنیت نقل و انتقال
وزن نهایی	۰/۲۶۶	۰/۲۰۴	۰/۲۹۷	۰/۱۹۳	۰/۱۱۱	۰/۱۰۷	۰/۱۴۲
اولویت	۲	۳	۱	۴	۶	۷	۵

زیرشاخص‌های امنیت داده	محرمانگی	جامعیت	بررسی هویت	سطح دسترسی	تشخیص و شناسایی	امنیت نقل و انتقال	سیاست امنیتی	دسترس پذیری
وزن نهایی	۰/۳۴۲	۰/۱۷۲	۰/۰۶۸	۰/۰۷۴	۰/۰۷۳	۰/۰۵۴	۰/۰۸۱	۰/۱۳۵
اولویت	۱	۲	۷	۵	۶	۸	۴	۳

امنیت برنامه‌های کاربرد	محرمانگی	جامعیت	بررسی هویت	سطح دسترسی	تشخیص و شناسایی	سیاست امنیتی	ممیزی و نظارت	دسترس پذیری
وزن نهایی	۰/۳۰۱	۰/۱۴۵	۰/۱۳۲	۰/۰۹	۰/۰۴۸	۰/۰۷۵	۰/۰۳	۰/۱۷۹
اولویت	۱	۳	۴	۵	۷	۶	۸	۲

امنیت در سطح مدیریت	مدیریت سیاست	مدیریت ریسک	مدیریت سیاست امنیتی
وزن نهایی	۰/۵۳۹	۰/۲۳۹	۰/۱۶۹
اولویت	۱	۲	۳

امنیت منابع فیزیکی	تجهیزات	کنترل عمومی
وزن نهایی	۰/۸۳۳	۰/۱۶۷
وزن نهایی	۱	۲
زیرشاخص‌های معماری	**ESB**	**پروکسی**
وزن نهایی	۰/۱۴۹	۰/۱۶
اولویت	۲	۱

همان‌طور که مشاهده می‌شود، در سطح ابعاد امنیتی، بیشترین اوزان به امنیت سطح داده و امنیت در طراحی معماری و کمترین اوزان به امنیت منابع انسانی اختصاص یافته است. بنابراین می‌توان نتیجه گرفت که امنیت سطح داده، بالاترین اهمیت و بیشترین تأثیر را در برقراری امنیت SOA دارد. در سطح زیر ابعاد مربوط به امنیت شبکه و وب، محکم کردن پایه‌های امنیتی اجزا، مجزا کردن فضای آدرس از فرآیندهای دیگر بیشترین میزان تأثیر را در برقراری امنیت شبکه داشته‌اند و کنترل ترافیک بین شبکه، امنیتIP ، امنیت نقل و انتقال، کشف و جلوگیری از تجاوز و حفاظت در مقابل حمله‌ها، به‌ترتیب در اولویت‌های بعدی قرار دارند.

در اولویت‌بندی زیر ابعاد مربوط به امنیت داده، محرمانگی، تمامیت، دسترس‌پذیری بالاترین تأثیر؛ در بخش امنیت برنامه‌های کاربردی، محرمانگی، دسترس‌پذیری؛ در قسمت پیاده‌سازی معماری، پروکسی؛ در برقراری امنیت در سطح مدیریت، مدیریت سیاست؛ در امنیت منابع انسانی، آموزش و در قسمت امنیت منابع فیزیکی، تجهیزات بیشترین تأثیر را در برقراری امنیت معماری سرویس‌گرا دارند.

در یک جمع‌بندی کلی از نتایج حاصل از داده‌های پژوهش، راهکارهای امنیتی SOA را می‌توان به دو دسته کلی تقسیم کرد. این نتایج به‌طور خلاصه در جداول شماره ۶ و ۷ نشان داده شده است.

جدول ٦. راهکارهای امنیتی مشابه با سایر سیستم‌های اطلاعاتی

تحصیل (Jonnaganti,2009)	**امنیت در بخش انسانی**
آموزش (Jonnaganti,2009)	
آگاهی(Jonnaganti,2009)	
استفاده از استاندارد WS-security policy(Ashley & Buecker, 2007)	**امنیت سیاست‌های امنیتی**
استفاده از تجرید یا انتزاع در طراحی سیاست‌ها (Ashley & Buecker, 2007)	
استفاده از استاندارد WS-addressing (Ashley & Buecker, 2007)	**امنیت در سطح نقل و انتقال**
استفاده از استاندارد WS-reliable messaging(Ashley & Buecker, 2007)	
استفاده از پروتکل SSL/TLS وS-HTTP (Ashley & Buecker, 2007)	
استفاده از شناسه کاربری، کلمه عبور، اثر انگشت (Ashley & Buecker, 2007)	**امنیت برای احراز هویت**
اصول رمزنگاری با کلید عمومی و خصوصی (Ashley & Buecker, 2007)	
استفاده از سرویس‌دهنده راهنما (Ashley & Buecker, 2007)	
استفاده از توکن‌های امنیتی (Ashley & Buecker, 2007)	

ادامه جدول ٦. راهکارهای امنیتی مشابه با سایر سیستم‌های اطلاعاتی

تعیین سطح دسترسی	دسته‌بندی‌کردن کاربردها، دیتابیس‌ها و روش‌های مشابه (Ashley & Buecker, 2007)
	استفاده از تکثیر سرویس‌ها (Ashley & Buecker, 2007)
جامعیت	استفاده از امضای دیجیتالی(Jonnaganti,2009)
	استفاده از پروتکل نقل و انتقالSSL/TLS (Ashley & Buecker, 2007)
محرمانگی	استفاده از استانداردXML encryption (Ashley & Buecker, 2007)
	استفاده از تکنیک‌های رمزگذاری(Jonnaganti, 2009)
	استفاده از پروتکل نقل و انتقالSSL/TLS (Ashley & Buecker, 2007)
امنیت شبکه	امنیت IP (Weily& Wing, 2005)
	فایروال‌های سخت‌افزار(Menzel,2007)
	ارزیابی آسیب‌ها (اسکن منظم سیستم‌های شبکه و زیرساختار) (Ashley & Buecker, 2007)
	سیاست‌های امنیتی ورود کاربر (Ashley & Buecker, 2007)
	پروکسی (Ashley & Buecker, 2007)
	سیستم‌های کشف وضعیت‌های نامطلوب(ADS) (Ashley & Buecker, 2007)
	سیاست‌های ایزولاسیون شبکه‌ها (Ashley & Buecker, 2007)

جدول ۷. راهکارهای امنیتی مختصSOA

امنیت در بخش طراحی و پیاده سازی	استفاده از پروکسی، برای اداره کردن امنیت HTTP/S و برای مجزا کردن تماس میان فراهم کننده و مشتری سرویس (Menzel, 2007)
	استفاده از گیت وی برای اداره کردن امنیتXML (Menzel, 2007)
	استفاده از گذرگاه سرویس سازمانی برای اجرای کنترل‌های امنیتی (Menzel, 2007)
برقراری امنیت بین مرزهای سازمانی	استفاده از پروکسی برای کنترل کردن امنیت درخواست‌های مبتنی بر پروتکل نقل و انتقالHTTP (Menzel, 2007) استفاده از گیت وی برای بررسی و کنترل درخواست‌هایSOAP (Menzel, 2007) مدیریت کردن سیاست‌های معتبر و هویت‌های یکپارچه شده بین مرزهای سازمان (Menzel, 2007)
امنیت سرویس‌های ترکیبی	استفاده از یک سیاست امنیتی مجزا برای سرویس‌های ترکیب شده (Afshar & Kavantzas, 2006)
	مدیریت کردن سیاست‌های معتبر و هویت‌های یکپارچه شده بین مرزهای سازمان (Afshar & Kavantzas, 2006)
امنیت در سطح پیام	حفاظت از بخش‌های مختلف پیام، به‌گونه‌ای که در مسیر پیام تنها توسط بخش‌هایی که مورد نظر است، قابل استفاده باشد (Afshar & Kavantzas, 2006)
	استفاده از استانداردWS-security (Menzel,2007)

نتیجه‌گیری و پیشنهادها

برای برقراری امنیت در هر سیستم اطلاعاتی، مدیران و دست‌اندرکاران برقراری امنیت، باید ابعاد و جنبه‌های مختلف امنیتی را مورد توجه قرار دهند، به‌گونه‌ای که در ایجاد یک سیستم اطلاعاتی ایمن به آنها کمک کند. در یک مقایسه کلی، تفاوت نتایج این پژوهش با پژوهش‌های پیشین در این است که با رویکردی متفاوت به مقوله امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا نگریسته شده است. این پژوهش برخلاف اکثر پژوهش‌ها، به‌جای بررسی امنیت از یک جنبه خاص و با یک رویکرد فنی، از دید سیستمی و مدیریتی به بررسی تمامی ابعاد و جنبه‌های امنیتی مورد نیاز یک مدیر IT که 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. در این پژوهش هفت بُعد مختلف امنیتی در یک سیستم اطلاعاتی سرویس‌گرا مورد بررسی قرار گرفته است. با توجه به اینکه تمام فرضیه‌های این پژوهش در سطح اطمینان ۹۵درصد مورد تأیید قرار گرفتند، می‌توان ادعا کرد که برقراری امنیت در سطح مدیریت، امنیت در سطح معماری، امنیت در سطح شبکه و وب سرویس، امنیت در سطح برنامه‌های کاربردی، امنیت در سطح منابع فیزیکی و محیط، امنیت در سطح منابع انسانی و امنیت در سطح داده، می‌توانند به‌منزله ابعاد (شاخص‌های) 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 می‌توان به دو دسته کلی تقسیم کرد.

دسته اول راهکارهایی است که مشابه راهکارهای امنیتی در سایر سیستم‌های 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-security برای امنیت سطح پیام و مانند آنها. انتظار ما بر این است که این ابعاد امنیتی و راهکارهای ارائه شده، تا اندازه‌ای به تصمیم‌گیری بهتر مدیران و مجریانی مسئول برقراری امنیت در سیستم‌های اطلاعاتی با معماری سرویس‌گرا کمک کند و بتواند امنیت را در سیستم‌های اطلاعاتی توسعه‌یافته با معماری سرویس‌گرا تا حد زیادی برقرار کند.

با توجه به ویژگی خاص معماری سرویس‌گرا از جمله سیستم‌های توزیع شده، داشتن مرزهای باز و تعامل با سرویس‌های بیرونی، به تمامی مدیرانی که در این حوزه مشغول فعالیت هستند پیشنهاد می‌شود:

۱. در هنگام تدوین سیاست‌های امنیتی، به‌ویژه سیاست‌های امنیتی مربوط به کنترل دسترسی و سیاست‌های مربوط به سرویس‌های ترکیبی که گاهی از ترکیب سرویس‌های 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, SOAP) می‌شود، توجه کافی داشته باشند. همچنین علاوه‌بر کنترل دسترسی با استفاده از فهرست راهنما، روش‌های دیگر کنترل دسترسی (مانند مدل کنترل دسترسی مبتنی بر رول) را مد نظر قرار دهند.

منابع

ایزدی، م. (۱۳۸۹). *امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با روش معماری سرویس‌گرا*. پایان‌نامه کارشناسی ارشد رشته مدیریت فناوری اطلاعات، دانشکده مدیریت، دانشگاه علامه طباطبایی.

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

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.

Hafner, M. (2009). Security Engineering for Service-oriented Architecture. *6th IEEE* International Conference Web Services, 6-8 February, Heidlelberg, Germany.

Hammar, K. (2006). *Towards a Stochastic Model for Integrated Security and Depend Ability Evaluation*. Proceeding of the 9th International Conference on Availability, Reliability and Security, 3-5July, Washington.

Hangjung, Z., Nazareth, D. (2010). Security and Performance in Service-oriented Application: Trading off Competing Objectives. *Decision support system*, 50(8) 336-346.

Heather, H., Hondo, M. (2005). Security Patterns within a Service-Oriented Architecture. *International Journal of Information Security*, 7(3): 23-34.

Jonnaganti, V. (2009). *An integrated Security Model for the Management of SOA.* Master Thesis Work in Software Engineering and Management.

Menzel, M. (2007). SOA Security- secures Cross- Organizational Service Composition. *Stuttgarter Software Technik Forum*, 21(4): 41-53.

Rosado, D. Eduardo, F. (2011). Security Services Architecture for Secure Mobile Grid Systems. *Journal of Systems Architecture: the EUROMICRO Journal*, 57(5): 240-258.

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.

xiaoming, B. (2006). *the Study on Secure Distributed Workflow Architecture Based SOA*. Proceeding of the 4th International Conference on Power System Technology, 8-10july, florida.

Yamany, H., Miriam, C. (2010). Intelligent Security and Access Control Framework for Secure-Oriented architecture. *Information and Software Technology*, 25 (2): 220-236.

Yue, H. & Tao, X. (2012). *Web Services Security Problem Insecure-oriented Architecture.* International Conference on Applied Physics and Industrial Engineering, 24(6): 1635-1641.