دانشگاه پیام نور
دانشکدهٔ فنی و مهندسی

پایان‌نامه
برای دریافت درجهٔ کارشناسی ارشد
رشتهٔ مهندسی‌کامپیوتر - گرایش نرم‌افزار
گروه فناوری اطلاعات و ارتباطات

ارائه یک چارچوب ارزیابی امنیت برای مدیریت و نظارت بر معماری سرویس گرا

حمیدرضا سلطانی

استاد راهنما:
دکتر سید مهران شرفی

استاد مشاور:
دکتر سید علی رضوی ابراهیمی

اسفند ۱۳۹۰

دانشگاه پیام نور
دانشکدهٔ فنی و مهندسی
دانشگاه پیام نور مرکز تهران

پایان‌نامه
برای دریافت درجه کارشناسی ارشد
رشتهٔ مهندسی کامپیوتر -گرایش نرم‌افزار
گروه فناوری اطلاعات و ارتباطات

ارائه یک چارچوب ارزیابی امنیت برای مدیریت و نظارت بر معماری سرویس گرا

حمیدرضا سلطانی

استاد راهنما:
دکتر سید مهران شرفی

استاد مشاور:
دکتر سید علی رضوی ابراهیمی

اسفند ۱۳۹۰

تقدیم به

همسر مهربانم که همواره پشتیبان من در این راه بود

و تقدیم به امیدهای زندگیم؛ نگین و متین که با لطافت
کودکانشان روشنی بخش زندگیمان هستند

و تقدیم به پدر و مادر بزرگوارم که با همتی بلند و راسخ حامی و
مشوقی برای ادامه تحصیلات من بوده اند

تشکر و قدردانی:

از زحمات و راهنمایی های استاد گرامی
جناب آقای دکتر مهران شرفی که در طول مدت انجام پایان نامه صبورانه و با دقت راهنمای بنده بوده اند صمیمانه تشکر دارم

از جناب آقای دکتر علی رضوی ابراهیمی بخاطر عنایت و رهنمودهای ارزشمندشان کمال تشکر را دارم.

چکیده

امروزه سازمانها برای همکاری و یکپارچگی سیستم های خود و بمنظور بقاء و موفقیت در محیط کسب و کار پویا از اصول معماری سرویس‌گرا بهره می برند که میزان این گرایش با توجه به ویژگیهای قابل توجه معماری سرویس گرا ازجمله اتصال سست، تعامل‌پذیری و استفاده مجدد در حال افزایش است. اما همین ویژگی‌ها در معماری سرویس‌گرا چالش ها و مشکلاتی را پیش روی این سیستم ها و فناوری‌ها قرار داده است که از جمله آن می‌توان به جنبه امنیت اشاره نمود. بنابراین بررسی راهکارها و مدل‌های امنیتی موجود در زمینه معماری سرویس گرا و ارائه یک چارچوب امنیتی بهبودیافته با رویکرد ارزیابی امنیت ضروری بنظر می‌رسد. علی رغم تلاشهایی که برای ارائه الگوها و مدل‌های امنیتی جامع برای SOA شده است، در حال حاضر هنوز فقدان یک ساختار امنیتی جامع برای چارچوب های مختلف سیستم‌های وسیع SOA که البته ویژگی سادگی فهم معنایی آن را دارا باشد وجود دارد. لذا هدف اصلی این تحقیق برای آدرس‌دهی این نیازها، ارائه یک چارچوب بهبودیافته برای تضمین امنیت SOA و در نتیجه بهبود تحلیل و نظارت بر آن می‌باشد. چارچوب ارائه شده از تکنیک‌های مهندسی معکوس ترکیب شده با پایگاه دانش امنیت بهره می‌برد که با تقویت پایگاه دانش با استفاده از تجربیات امنیتی بدست آمده و نیز بهره مندی از معیارهای اندازه‌گیری و اصول وزندهی فرآورده‌های امنیتی، باعث تقویت قدرت تحلیل و ارزیابی امنیت می‌شود.

واژه های کلیدی: ارزیابی امنیت، معماری سرویس گرا، چارچوب ارزیابی امنیت، پایگاه دانش امنیت، تحلیل امنیت، مدیریت و نظارت امنیت

فهرست مطالب

عنوان **صفحه**

فهرست اشکال

عنوان **صفحه**

فهرست جداول

فهرست علائم اختصاری

ACL	Access Control List	لیست کنترل دسترسی
BI	Business Intelligence	کسب و کار هوشمند
BPM	Business Process Management	مدیریت فرایندهای کسب
CIA	Confidentiality, Integrity and Availability	قابلیت اعتماد، یکپارچگی و دسترس پذیری
EAI	Enterprise Application Integration	یکپارچه سازی برنامه کاربردی سازمان
EMF	Eclipse Modeling Framework	چارچوب مدلسازی اکلیپس
ERP	Enterprise Resource planning	برنامه ریزی منابع سازمانی
ESB	Enterprise Service Bus	گذرگاه سرویس سازمانی
J2EE	Java 2 Enterprise Edition	نسخه دوم سازمانی جاوا
JDT	Java Development Tools	ابزارهای توسعه جاوا
LDAP	Lightweight Directory Access Protocol	پروتکل دستیابی فهرست سبک وزن
RBAC	Role-Based Access Control	کنترل دسترسی نقش-محور
SAML	Security Assertion Markup Language	زبان نشانه گذاری تأیید امنیت
SAVE	Software Architecture Visualization and Evaluation	ارزیابی و مجازی سازی معماری نرم افزار
SCA	Service Component Architecture	معماری مؤلفه سرویس
SOA	Service Oriented Architecture	معماری سرویس گرا
SOAP	Simple Object Access Protocol	پروتکل دسترسی آسان به اشیأ

SSL	Secure Socket Layer	لایه سوکت امن
TLS	Transform Layer Security	امنیت سطح انتقال
UDDI	Universal Description Discovery and Integration	توصیف، کشف و یکپارچه سازی فراگیر
WSDL	Web services description language	زبان توصیف سرویس ها وب
XML	Extensible Markup Language	زبان نشانه گذاری توسعه یافته

فصل۱

مقدمه

۱-۱. مقدمه

معماری سرویس گرا[1] یک چارچوب وسیع و استاندارد برای ساخت سیستم‌های توزیع شده ناهمگن است که کارکردهای نرم افزاری را در قالب سرویس ارائه می‌کند و تضمین کننده توسعه و یکپارچگی سیستم هاست و هدفش افزایش چابکی[2] فناوری اطلاعات در جهت واکنش سریع به تغییرات در نیازهای کسب و کار است. این سرویس‌ها هم توسط دیگر نرم افزارها قابل فراخوانی هستند و هم برای ساخت سرویس‌های جدید مورد استفاده قرار می‌گیرند.

تکامل و رشد معماری سرویس‌گرا در واقع بیانگر نوعی تبدیل و تحول در کسب و کار و فناوری است. فرصت‌های بوجود آمده از معماری سرویس‌گرا امکان ظهور و پیدایش بالقوه سازمان‌هایی را فراهم می سازد که تمام قابلیت‌هایشان به کمک سرویس ها و بعضاً بصورت خودکار پیاده سازی شده‌اند. در این سازمان‌ها فرایندها از مرزهای آن ها فراتر رفته و بین فراهم کنندگان مواد اولیه، مشتریان و کلیه شرکا ارتباط برقرار می کنند تا زنجیره‌های ارزش سازمان‌ها کاراتر از گذشته شکل گیرند.

سرویس‌های وب[3] را باید نوعی فناوری برای تحقق ویژگی استقلال از سکو و ابزاری برای پیاده سازی معماری سرویس‌گرا دانست. یک سرویس وب بهترین راه حل برای پیاده سازی معماری سرویس‌گرا است (الواسی[4]، ۲۰۰۸).

---

[1] Service Oriented Architecture (SOA)
[2] agility
[3] web services
[4] Oluwaseyi

۱-۲. تعریف مسئله و سؤالات اصلی تحقیق

نیازمندی‌های حیاتی امنیت برای محفوظ نگهداشتن یک سیستم اطلاعاتی عبارتند از قابلیت اعتماد، یکپارچگی و دسترس پذیری (CIA[1]). اما درمورد SOA نیازمندیهای اضافی دیگری چون اعتبارسنجی[2]، تعیین اختیارات[3]، حسابرسی[4] و رد انکار[5] داریم.

در چارچوب ارائه شده در این تحقیق از ترکیب تکنیک‌های مختلفی برای ارزیابی امنیت یک سیستم معماری سرویس گرا استفاده شده است، که از آن جمله می‌توان به *تحلیل استاتیک* و *تکنیک‌های مهندسی معکوس* جهت جمع‌آوری اطلاعات مرتبط با امنیت و گردآوری دانش مربوط به نیازمندیهای امنیتی سیستم در یک *پایگاه دانش* اشاره نمود. کارهای بسیاری در زمینه تحلیل استاتیک نرم افزار انجام شده است، مانند (هاورمایر[6]، ۲۰۰۴) و (لیوشیتز[7]، ۲۰۰۵، ۲۰۰۶). برای ارزیابی امنیت یک سیستم نرم افزاری در (جانگ[8]، ۲۰۱۱) از روش تحلیل استاتیک استفاده شده که جهت تقویت آن از یک مدل پایگاه دانش بهره گرفته شده است. ارزیابی امنیت یک صفت کیفی مشخص در یک سطح معماری هنوز در ابتدای راه است. *روش های پشتیبانی شده با ابزار* کمی وجود دارند که امنیت را در سطوح بالاتر تجرید نسبت به کد منبع[9] توسعه دهند. در (سهر و برگر[10]، ۲۰۱۰) یک روش معماری مرکزی برای تحلیل امنیت استاتیک معرفی شده است که از یک ابزار مهندسی معکوس جهت استخراج اطلاعات ساختاری از کد منبع استفاده شده است.

---

[1] Confidentiality, Integrity and Availability
[2] authentication
[3] authorization
[4] accountability
[5] non-repudiation
[6] Hovemeyer
[7] Livshits
[8] Jung
[9] source code
[10] Sohr, B. Berger

سؤال‌های اصلی مطرح شده عبارتند از:

- آیا قدرت تحلیل و ارزیابی امنیت در چارچوب ارائه شده تقویت شده است؟
- چارچوب پیشنهادی چگونه و تا چه اندازه امنیت را در سطح معماری سرویس‌گرا تأمین می‌کند؟
- آیا برای غیر متخصصان یا کاربران کم تجربه در زمینه امنیت، قابل فهم و ساده است؟
- آیا ابزار ارزیابی چارچوب پیشنهادی مستقل از زبان برنامه نویسی و فناوری است؟

۱-۳. سابقه و ضرورت انجام تحقیق

امروزه سازمانها برای همکاری و یکپارچگی سیستم‌های خود و بمنظور بقاء و موفقیت در محیط کسب و کار پویا از اصول معماری سرویس‌گرا بهره می‌برند که میزان این گرایش با توجه به ویژگی‌های قابل توجه معماری سرویس گرا ازجمله اتصال سست[1]، تعامل پذیری[2] و استفاده مجدد[3] در حال افزایش است. اما همین ویژگیها در معماری سرویس‌گرا چالش ها و مشکلاتی را پیش روی این سیستم‌ها و فناوری‌ها قرار داده است که از جمله آن می‌توان به جنبه *امنیت* اشاره نمود. بنابراین بررسی راهکارها و مدل‌های امنیتی موجود در زمینه معماری سرویس‌گرا و ارائه یک چارچوب امنیتی بهبودیافته با رویکرد ارزیابی امنیت ضروری بنظر می‌رسد. متأسفانه آزمایش کیفیت جنبه امنیت سیستم‌های نرم افزاری امر ساده‌ای نمی‌باشد. تاکنون تلاشهایی برای ارائه الگوها و مدل‌های امنیتی جامع برای SOA شده است و مقالات، پایان نامه ها و چندین کتاب توسط محققان و مؤلفان در این باره عرضه شده است. با این حال در حال حاضر

[1] loosely coupling
[2] interoperability
[3] reusability

هنوز فقدان یک شیوه جامع که یک توسعه و پیشرفت قاعده منـد در سـاختار امنیـت SOA را ارائه دهد و البته ویژگی سادگی فهم معنایی آن را دارا باشد وجود دارد. اگرچـه اسـتانداردهای فنی نظیر امنیت وب سرویس (فرناندز[1] و همکاران، ۲۰۰۶) موجود اسـت، سیسـتم هـای SOA هنوز در برابر بسیاری از انواع تهدیدهای اساسی آسیب پذیرند.

لذا هدف اصلی این تحقیق برای آدرس‌دهی این نیازها، ارائه یک چارچوب بهبودیافته برای تضمین امنیت SOA و در نتیجه بهبود نظارت بر آن می‌باشد.

۱-۴. اهداف تحقیق

کلیه سازمان‌ها و سیستم های فناوری اطلاعات در سراسر دنیا در حـال حرکـت سـریع بـه سمت معماری سرویس‌گرا هستند. بدیهی است که جوانب امنیت در SOA از مهمترین اهـداف مدیران سازمان‌ها جهت مدیریت و نظارت هرچه بهتر سیستم‌ها خواهد بود. هـدف اصـلی ایـن تحقیق ارائه یک چارچوب امنیتی بهبودیافته برای مدیریت و نظارت بـر معمـاری سـرویس‌گـرا می‌باشد. با توجه به اهمیت موضوع اهداف جانبی زیادی می‌توان برای این تحقیـق برشـمرد. از آن جمله می‌توان به موارد زیر اشاره نمود:

- ارائه چارچوبی یکپارچه برای ارزیابی امنیت سیستم‌های سرویس‌گرا که مستقل از فناوری و زبان برنامه نویسی خاصی باشد.
- استفاده از یک مدل *پایگاه دانش*[2] در طول مدت فرایند تحلیل و ارزیابی امنیت، جهت بروز رسانی و غنی‌سازی دانش امنیت، با هدف سازگاری با نیازمندیهای امنیتی جدید سیستم و قابلیت توسعه برای پرداختن به مسائل ارزیابی جدید در آینده.

[1] Fernandez
[2] Knowledge Base

۱-۵. فرضیه ها

- در چارچوب پیشنهادی از تکنیک‌های مهندسی معکوس ترکیب شده با پایگاه دانش جهت تقویت ارزیابی امنیت استفاده شده است.
- تقویت پایگاه دانش با استفاده از تجربیات امنیتی بدست آمده باعث تقویت قدرت تحلیل و ارزیابی امنیت می‌شود.
- قابلیت و کیفیت چارچوب پیشنهادی بستگی دارد به کیفیت قواعد برچسب[1] امنیتی و کامل بودن اطلاعات فراهم شده در پایگاه دانش.

فرضیه‌های فرعی:

- برای تحقق فرضیات اصلی، نیازمند داشتن دانش کافی درمورد ابزارها، استانداردها و فناوریهای مرتبط با موضوع هستیم.

۱-۶. روش انجام تحقیق

معماری سرویس‌گرا، امنیت و کاربرد امنیت در معماری سرویس‌گرا کم و بیش درک شده‌اند. جهت ارزیابی موضوع، تحقیق باید تکنیک‌های مرتبط مجزا را درجهت یک راه حلی که امنیت را در SOA مهیا می‌کند ترکیب نماید.

نوع روش تحقیق مطالعه کتابخانه‌ای (منابع تحقیقاتی معتبر و استانداردهای جهانی) در جهت تحقق اهداف ذیل می‌باشد:

- شناخت و درک اصول معماری سرویس گرا (با مروری بر ادبیات موضوع).

[1] tag