

دانشگاه صنعتی امیرکبیر

دانشکده مهندسی کامپیوتر و فناوری اطلاعات

پایان نامه کارشناسی ارشد

در رشته مهندسی کامپیوتر، گرایش نرم افزار

موضوع:

روشی نو برای مدلسازی و ارزیابی ویژگی های کیفی (نیازهای غیرکارکردی)

در معماری نرم افزار

نگارش :

پویا جافریان

استاد راهنما :

دکتر احمد عبدالله زاده بارفروش

مرداد ۸۶



دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)
معاونت پژوهشی

بسمه تعالی

فرم اطلاعات پایان نامه

کارشناسی ارشد و دکترا

تاریخ: ۸۶/۶/۱۴

پیوست:

نام و نام خانوادگی: پویا جعفریان

دانشجوی آزاد

بورسیه

معادل

شماره دانشجویی: ۸۴۱۳۱۰۷۱

دانشکده: مهندسی کامپیوتر رشته تحصیلی: مهندسی کامپیوتر، گرایش نرم افزار

نام و نام خانوادگی استاد راهنما: دکتر احمد عبدالله زاده بارفروش

عنوان پایان نامه به فارسی: روشی نو برای مدلسازی و ارزیابی ویژگی های کیفی (نیازهای غیر کارکردی) در معماری نرم افزار

عنوان پایان نامه به انگلیسی: A New Approach for Modeling and Evaluation of Quality Attributes (Non-functional Requirements) in Software Architecture

کارشناسی ارشد

نوع پروژه: کاربردی بنیادی توسعه ای نظری

دکترا

تعداد واحد: ۶ واحد

تاریخ خاتمه: ۸۶/۶/۱۰

تاریخ شروع: ۸۵/۷/۱

سازمان تامین کننده اعتبار:

واژه های کلیدی به فارسی: مدلسازی ویژگی های کیفی، مدیریت اعتماد، کنترل دسترسی، معماری نرم افزار

واژه های کلیدی به انگلیسی: Modeling Quality Attributes, Trust Management, Access Control, Software Architecture

نظرها و پیشنهادها به منظور بهبود فعالیت های پژوهشی دانشگاه:

استاد راهنما:

دانشجو:

امضاء استاد راهنما: تاریخ:

نسخه ۱: معاونت پژوهشی

نسخه ۲: کتابخانه و به انضمام دو جلد پایان نامه به منظور تسویه حساب با کتابخانه و مرکز اسناد و مدارک علمی

تقدیم به پدر و مادر عزیزم، که همواره پشتیبان و حامی من بوده اند.

تقدیم به برادر عزیزم کوشا، با آرزوی موفقیت های هرچه بیشتر

تشکر و قدردانی

در ابتدا لازم می‌دانم از استاد راهنمای خود، جناب آقای دکتر عبداله‌زاده، به پاس راهنمایی‌های ارزنده ایشان در طول تحصیل در دانشگاه صنعتی امیرکبیر، تشکر و قدردانی نمایم.

از اساتید محترم داور، جناب آقای دکتر صادقیان و جناب آقای دکتر حبیبی، برای قبول داوری این پایان نامه و مطالعه آن کمال تشکر را دارم.

همچنین از آقایان پژمان صالحی و وحید کاظم پور و خانم آزاده نعمت زاده، که در شروع پروژه همکاری‌های زیادی را با من انجام دادند، و خانم سارا مطیعی که در تهیه پایان نامه با من همکاری نمودند، سپاسگزارم.

هدف اصلی مهندسی نرم افزار، تولید سیستم با کیفیت است. اولین مرحله ای که کیفیت یا ویژگی های کیفی در آن مورد توجه قرار می گیرد، مرحله تولید معماری نرم افزار سیستم می باشد. در این مرحله، نیازهای کیفی و تاکتیک های برآورده کننده آنها مدل شده و مورد ارزیابی قرار می گیرند. هدف این پایان نامه ارائه رویکردی جدید برای حل مسئله مدلسازی ویژگی های کیفی در معماری نرم افزار می باشد. برای ارائه این رویکرد، بر پایه چارچوب ISLab، مراحل ایجاد یک روش مدلسازی جدید، برای مدل نمودن مدیریت اعتماد در سطح معماری نرم افزار نشان داده خواهد شد. مدیریت اعتماد، یکی از تاکتیک های دستیابی به امنیت بوده و با مدلسازی آن، امکان ارزیابی میزان دستیابی به امنیت در معماری نرم افزار فراهم می گردد. مهمترین خروجی پژوهش انجام شده، یک زبان مدلسازی گسترش یافته بر پایه UML به نام UMLTrust بوده که توانایی مدلسازی مدیریت اعتماد در سطح معماری نرم افزار را دارا است. همچنین مدل های ایجاد شده توسط UMLTrust، مدل هایی با قابلیت ارزیابی می باشند.

واژه های کلیدی: مدلسازی ویژگی های کیفی، مدیریت اعتماد، کنترل دسترسی، معماری نرم افزار.

فهرست مطالب

۷	فصل ۱ مقدمه
۸	۱-۱ مقدمه
۱۲	۲-۱ رویکرد حل مسئله
۱۲	۳-۱ مهمترین دستاوردهای پروژه
۱۳	۴-۱ ساختار پایان نامه
۱۴	فصل ۲ ویژگیهای کیفی در معماری نرم افزار
۱۵	۱-۲ مقدمه
۱۵	۲-۲ معماری نرم افزار
۱۷	۳-۲ ارتباط معماری نرم افزار و ویژگیهای کیفی
۱۸	۴-۲ اندازه ها، متریک ها و شاخص ها
۱۹	۵-۲ سناریوهای ویژگی کیفی
۲۱	۶-۲ دستیابی به ویژگیهای کیفی
۲۱	۱-۶-۲ تاکتیکهای معماری
۲۲	۲-۶-۲ الگوهای معماری
۲۲	۳-۶-۲ مدلسازی تاکتیک ها و الگوهای معماری
۲۳	۷-۲ فرایند کلی مدلسازی و ارزیابی ویژگیهای کیفی در معماری نرم افزار
۲۵	۱-۷-۲ امکان سنجی ویژگی های کیفی
۲۶	۸-۲ نتیجه گیری
۲۸	فصل ۳ مفاهیم پایه امنیت و کارهای انجام شده
۲۹	۱-۳ مفاهیم پایه امنیت
۲۹	۱-۱-۳ مروری بر امنیت
۳۰	۲-۱-۳ مدل های امنیتی
۳۸	۲-۳ جایگاه کار ارائه شده در امنیت
۴۰	۳-۳ کارهای انجام شده
۴۱	۱-۳-۳ مدل فرایند
۴۳	۲-۳-۳ مدلسازی کنترل دسترسی در سیستم های امن
۵۰	۳-۳-۳ مدلسازی کنترل دسترسی با زبان های غیر UML
۵۱	۴-۳ مقایسه روش های ارائه شده
۵۳	۵-۳ نتیجه گیری
۵۴	فصل ۴ زبان UMLTrust
۵۵	۱-۴ مقدمه
۵۷	۲-۴ مفاهیم پایه

۵۷.....	۱-۲-۴ عناصر اصلی مدل‌سازی مدیریت اعتماد در چارچوب RT.....
۶۰.....	۲-۲-۴ مدل‌سازی یک سیستم نمونه به وسیله چارچوب RT.....
۶۰.....	۳-۲-۴ نقاط ضعف مدل‌سازی سیستم به وسیله چارچوب RT.....
۶۱.....	۳-۴ مدل‌سازی مدیریت اعتماد با زبان UML.....
۶۱.....	۱-۳-۴ متا مدل UML.....
۶۲.....	۲-۳-۴ رویکردهای ممکن برای گسترش UML در مسئله مدل‌سازی مدیریت اعتماد در سطح معماری.....
۶۶.....	۳-۳-۴ مکانیزم‌های گسترش زبان UML از طریق محدود کردن آن.....
۶۸.....	۴-۴ پروفایل UMLTrust برای مدل‌سازی مدیریت اعتماد در سطح معماری نرم افزار.....
۶۸.....	۱-۴-۴ مدل‌سازی موجودیت‌ها.....
۶۹.....	۲-۴-۴ مدل‌سازی نقش.....
۷۱.....	۳-۴-۴ مدل‌سازی رابطه اعطا کردن نقش به نقش (وکالت).....
۷۱.....	۴-۴-۴ مدل‌سازی رابطه "داشتن ویژگی".....
۷۲.....	۵-۴-۴ مدل‌سازی رابطه "مالکیت یک نقش".....
۷۳.....	۶-۴-۴ مدل‌سازی رابطه "عضویت".....
۷۴.....	۷-۴-۴ مدل‌سازی واسط‌ها.....
۷۵.....	۸-۴-۴ رابطه "دسترسی به یک واسط".....
۷۶.....	۹-۴-۴ خلاصه گسترش‌های ارائه شده.....
۷۸.....	۵-۴/ارزیابی مدل‌های ایجاد شده.....
۸۰.....	۶-۴ الگوهای معماری برای مدل‌سازی مدیریت اعتماد در سطح معماری نرم افزار.....
۸۰.....	۱-۶-۴ الگوی معماری برای نمایش عضویت یک جزء در یک نقش.....
۸۰.....	۲-۶-۴ الگوی معماری برای نمایش اعطا کردن یک نقش به نقش دیگر.....
۸۱.....	۳-۶-۴ الگوی نقش‌های سلسله‌مراتبی.....
۸۲.....	۴-۶-۴ الگوی معماری اعطا کردن چندگانه.....
۸۳.....	۷-۴/ارائه یک مثال برای مدل‌سازی به کمک UMLTrust.....
۸۶.....	فصل ۵ مطالعه موردی.....
۸۷.....	۱-۵ مقدمه.....
۸۷.....	۲-۵ تعریف مسئله.....
۸۷.....	۳-۵ حل مسئله.....
۸۸.....	۱-۳-۵ نیازمندی‌های مسئله.....
۸۹.....	۲-۳-۵ سناریو ویژگی کیفی.....
۹۰.....	۳-۳-۵ معماری کلی سیستم.....
۹۲.....	۴-۵ مدل‌سازی سیستم از دیدگاه مدیریت اعتماد.....
۹۲.....	۱-۴-۵ سناریو یک ، دسترسی رایگان برای دانشجویان و اساتید دانشکده.....
۹۳.....	۲-۴-۵ سناریو دو، امکان خریداری مقالات توسط دانشجویان دانشکده‌های دیگر.....
۹۶.....	فصل ۶ ارزیابی مبتنی بر ویژگی.....
۹۷.....	۱-۶ مقدمه.....

۶-۲ پارامترهای ارزیابی.....	۹۷
فصل ۷ نتیجه گیری و کارهای آینده.....	۱۰۲
فصل ۸ مراجع.....	۱۰۶

فهرست اشکال

شکل ۱-۱	تعداد آسیب پذیری های گزارش شده بر حسب سال توسط CERT/CC	۱۰
شکل ۲-۱	تعداد حملات گزارش شده بر حسب سال توسط CERT/CC	۱۰
شکل ۱-۲	بخش های تشکیل دهنده سناریو ویژگی کیفی [۱]	۲۰
شکل ۲-۲	نمونه ای از تاکتیک های معماری امنیت [۱]	۲۱
شکل ۳-۲	فرایند کلی مدل سازی و ارزیابی ویژگی های کیفی در معماری نرم افزار	۲۴
شکل ۱-۳	کنترل دسترسی مبتنی بر نقش (RBAC)	۳۳
شکل ۲-۳	اجزا تشکیل دهنده سیستم RBAC سلسله مراتبی	۳۴
شکل ۳-۳	جایگاه کار ارائه شده در درخت پژوهش امنیت	۳۹
شکل ۴-۳	جایگاه کار انجام شده در درخت پژوهش معماری نرم افزار	۳۹
شکل ۵-۳	مهندسی نرم افزار سیستم های امن به عنوان یک تکنولوژی لایه ای	۴۱
شکل ۱-۴	مراحل طی شده برای ایجاد زبان مدل سازی UMLTrust	۵۶
شکل ۲-۴	معماری چهار لایه UML در مدل سازی	۶۲
شکل ۳-۴	متا مدل UML که برای مدل سازی مدیریت اعتماد محدود شده است	۶۳
شکل ۴-۴	گسترش متامدل UML برای مدل سازی مدیریت اعتماد	۶۴
شکل ۵-۴	بخشی از متامدل UML	۶۸
شکل ۶-۴	گسترش کلاس UML برای مدل سازی جزء	۶۹
شکل ۷-۴	گسترش کلاس UML برای مدل سازی نقش	۶۹
شکل ۸-۴	گسترش Association در UML برای مدل سازی رابطه اعطا کردن	۷۱
شکل ۹-۴	گسترش Association در UML برای مدل سازی رابطه داشتن ویژگی	۷۲
شکل ۱۰-۴	گسترش Association در UML برای مدل سازی رابطه مالکیت نقش	۷۳
شکل ۱۱-۴	گسترش Association در UML برای مدل سازی رابطه عضویت	۷۴
شکل ۱۲-۴	گسترش واسط در UML برای مدل سازی واسط امن	۷۵
شکل ۱۳-۴	گسترش Association در UML برای مدل سازی رابطه دسترسی	۷۶
شکل ۱۴-۴	الگوی معماری عضویت در یک نقش	۸۰
شکل ۱۵-۴	الگوی معماری اعطا کردن یک نقش به نقش دیگر (اعتماد)	۸۱
شکل ۱۶-۴	الگوی معماری نقش های سلسله مراتبی	۸۲
شکل ۱۷-۴	الگوی معماری اعطا کردن چندگانه	۸۳
شکل ۱۸-۴	مدل سازی سناریو ارائه کد کاربری و کلمه عبور	۸۴
شکل ۱۹-۴	مدل سازی سناریو ارائه کد کاربری و کلمه عبور و قراردادن در زیرمجموعه امیر کبیر	۸۴

- شکل ۴-۲۰ مدل‌سازی سناریو مدیریت اعتماد ۸۵
- شکل ۵-۱ سناریو امنیت برای جلوگیری از دسترسی کاربران غیرعضو کتابخانه ۸۹
- شکل ۵-۲ سناریو امنیت برای جلوگیری از دسترسی فارغ التحصیلان ۸۹
- شکل ۵-۳ سناریو کارایی برای انتقال تغییرات ۸۹
- شکل ۵-۴ سناریو قابلیت استفاده در حذف یا اعطای دسترسی به کلیه اساتید یا دانشجویان ۸۹
- شکل ۵-۵ معماری متمرکز برای سیستم ارائه مقالات ۹۰
- شکل ۵-۶ معماری توزیع شده برای سیستم ارائه مقالات ۹۱
- شکل ۵-۷ مدل‌سازی سناریو دسترسی نامحدود دانشجویان و اساتید به سیستم ارائه مقالات ۹۴
- شکل ۵-۸ مدل‌سازی سناریو خرید مقالات برای اعضای دانشکده های دیگر ۹۵

فهرست جداول

جدول ۱-۲	ماتریس انتخاب موضوع برای انتخاب یکی از ویژگی های کیفی	۲۶
جدول ۱-۳	مقایسه فرایندهای مدلسازی سیستم های امن	۴۳
جدول ۲-۳	مقایسه روش های مدلسازی کنترل دسترسی و مدیریت اعتماد	۵۲
جدول ۱-۴	مقایسه سه رویکرد مختلف در استفاده از UML برای مدلسازی مدیریت اعتماد	۶۵
جدول ۲-۴	پروفایل گسترش های انجام شده (کلیشه ها)	۷۶
جدول ۳-۴	پروفایل گسترش های انجام شده (برچسب ها)	۷۷
جدول ۴-۴	نحوه نگاشت عناصر UMLTrust به RT	۷۸
جدول ۱-۵	نیازمندی های کارکردی مسئله	۸۸
جدول ۲-۵	نیازمندی های امنیتی مسئله	۸۸
جدول ۳-۵	نیازمندی های کارایی مسئله	۸۸
جدول ۴-۵	نیازمندی های قابلیت استفاده	۸۹
جدول ۱-۶	مقایسه روش های مدلسازی مدیریت اعتماد و کنترل دسترسی	۱۰۱

فصل ١ مقدمه

۱-۱ مقدمه

امروزه یکی از مهمترین ویژگی‌های هر سیستم نرم‌افزاری، کیفیت است. با پیشرفت‌های انجام شده و گسترش ابزارهای گوناگون برای توسعه نرم‌افزار، توسعه نرم‌افزارهایی که کارکردهای مورد نظر مشتریان را برآورده سازند، به امری آسان و سریع تبدیل شده است. در حال حاضر، تفاوت بین دو نرم‌افزار را توانایی نرم‌افزارها در برآورده ساختن ویژگی‌های کیفی مورد انتظار، تعیین می‌کند.

معماری نرم افزار یک برنامه یا سیستم کامپیوتری، ساختار یا ساختارهایی از سیستم می باشد، که در برگیرنده اجزاء، صفات قابل مشاهده آن اجزا و ارتباط بین آنها باشد [۱]. معماری نرم‌افزار یک سیستم نرم‌افزاری، شامل اولین تصمیمات طراحی سیستم می‌باشد و این تصمیمات زیربنای فعالیت‌های طراحی، پیاده‌سازی، استقرار و نگهداری سیستم است. همچنین معماری نرم‌افزار، اولین عنصر قابل ارزیابی در فرایند توسعه نرم‌افزار می‌باشد [۱]. بنابراین برای طراحی سیستمی که نیازهای کیفی مورد نظر را برآورده سازد، تولید معماری نرم‌افزار اولین گام در دستیابی به کیفیت در نرم‌افزار و همچنین ارزیابی ویژگی‌های کیفی است.

برای دستیابی به کیفیت در مدل‌های فرایند توسعه نرم‌افزار مبتنی بر معماری^۱، معمولاً ابتدا نیازهای کیفی سیستم به طور دقیق و قابل اندازه‌گیری تعیین شده و سپس معماری نرم‌افزار مربوطه طراحی می‌گردد. پس از طراحی معماری، می‌توان به ارزیابی آن پرداخت و تغییرات لازم را در طراحی مورد نظر ایجاد کرد. بنابراین دو مرحله اساسی در مدل‌های فرایند توسعه نرم‌افزار مبتنی بر معماری، مراحل طراحی و ارزیابی معماری نرم‌افزار است. این دو بخش در ارتباط مستقیم با یکدیگر بوده و هر یک مکمل دیگری می‌باشد. برای ایجاد امکان ارزیابی ویژگی‌های کیفی مورد نظر در معماری، در مرحله طراحی معماری، باید به ازای هر ویژگی کیفی، یک مدل از معماری نرم‌افزار ایجاد شود. این مدل‌ها نحوه دستیابی به ویژگی کیفی را نشان داده و با ارزیابی آن‌ها می‌توان مشخص نمود به چه میزان ویژگی کیفی مورد نظر برآورده شده است.

برای طراحی معماری نرم‌افزار، نیاز به تاکتیک معماری^۲ و الگوهای معماری^۳ است. برای برآورده ساختن ویژگی‌های کیفی در معماری نرم‌افزار، می‌توان تعدادی تاکتیک معماری معرفی کرد. این تاکتیک‌ها روش‌هایی در راستای برآورده کردن ویژگی کیفی مذکور هستند. به عنوان مثال، ویژگی

¹ Architecture Centric

² Architectural Tactics

³ Architectural Patterns

کیفی امنیت دارای تعدادی تاکتیک معماری بوده که ویژگی کیفی امنیت را در سطح معماری نرم افزار برآورده می کنند. به عنوان نمونه هایی از این تاکتیک ها می توان به تشخیص هویت کاربران، محدود کردن دسترسی کاربران، تشخیص نفوذ، کنترل دسترسی، مدیریت اعتماد و ... اشاره کرد که فهرست کامل این تاکتیک ها در بخش ۲-۶-۱ ارائه شده است.

در هنگام استفاده از تاکتیک های معماری در طراحی معماری نرم افزار، همانطور که اشاره شد، این تاکتیک ها باید مدل شوند. مدل نمودن تاکتیک ها به دلایل زیر انجام می شود:

۱. امکان ارزیابی تاکتیک استفاده شده و بررسی برآورده شدن نیازمندی مورد نظر
 ۲. مستند سازی تاکتیک های مورد استفاده، به گونه ای که امکان درک تاکتیک های استفاده شده به سادگی فراهم باشد.

۳. امکان استفاده از مدل ها برای شبیه سازی اجرای برنامه

۴. امکان تبدیل تاکتیک های ایجاد شده به محصولات نرم افزاری مراحل طراحی و پیاده سازی
 بنابراین منظور از مدلسازی ویژگی های کیفی در این پایان نامه، ایجاد مدلی از معماری بوده که بیانگر یک ویژگی کیفی باشد و نحوه دستیابی به ویژگی کیفی توسط یک تاکتیک مشخص در آن ارائه شده باشد. همچنین مدل ایجاد شده باید قابل ارزیابی باشد.

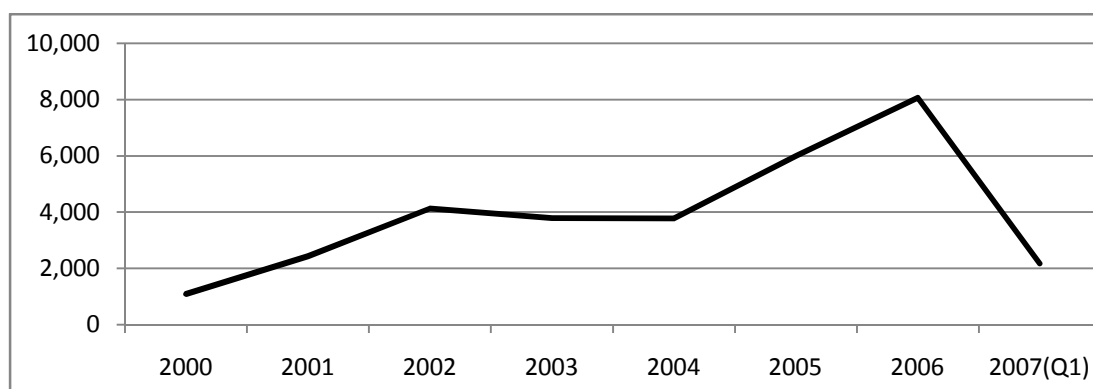
برای دستیابی به هدف مذکور، در این پایان نامه ویژگی کیفی امنیت انتخاب شده و روشی نو برای مدلسازی مدیریت اعتماد که یکی از تاکتیک های دستیابی به امنیت می باشد، ارائه شده است. اصلی ترین علت انتخاب امنیت به عنوان ویژگی کیفی نمونه در این پایان نامه، افزایش روزافزون نیاز به امنیت در سیستم های کامپیوتری بوده است.

در دهه اخیر، سیستم های کامپیوتری در سراسر دنیا و در جنبه های مختلف زندگی انسان، نفوذ کرده اند. در دنیای امروز، افراد و سازمان ها کار و زندگی خود را بر پایه قدرت پردازش و ارتباطی سیستم های کامپیوتری بنا نموده اند و با گذشت زمان نیز، وابستگی جوامع به سیستم های کامپیوتری روز به روز بیشتر خواهد شد.

در کنار بسیاری از ویژگی های مثبت و تاثیرات سیستم های کامپیوتری در دنیای امروز، وابستگی به این سیستم ها، اثرات منفی نیز به همراه دارد. یکی از اثرات منفی، گسترش روزافزون اشکالات امنیتی در سیستم های کامپیوتری و افزایش حملات علیه این گونه سیستم ها می باشد. موسسه ^۱CERT/CC

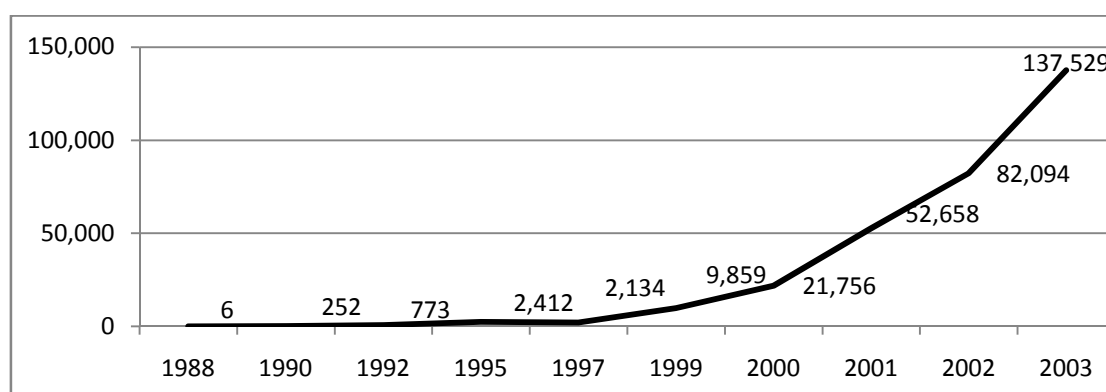
^۱ Computer Emergency Response Team Coordination Center

سالانه گزارش‌هایی مبنی بر تعداد آسیب پذیری^۱ های موجود در سیستم های کامپیوتری (آسیب پذیری ها اشکالات امنیتی هستند که به صورت رسمی و در مجامع عمومی گزارش داده می شوند). ارائه می‌دهد. بر اساس گزارش ارائه شده توسط این موسسه [۲] در سال ۲۰۰۶ بیش از ۸۰۰۰ آسیب پذیری در سیستم های کامپیوتری توسط منابع معتبر گزارش شده است و این مقدار سال به سال رو به افزایش است (شکل ۱-۱).



شکل ۱-۱ تعداد آسیب پذیری های گزارش شده بر حسب سال توسط CERT/CC

همچنین CERT/CC تعداد ۱۴۰۰۰۰ حمله امنیتی را در سال ۲۰۰۳ گزارش نموده است. تعداد این حملات سال به سال و به شدت رو به افزایش می باشد، به طوری که این موسسه از سال ۲۰۰۴ به بعد ارائه آمار در زمینه حملات امنیتی را متوقف نمود (شکل ۲-۱). باید توجه داشت که تعداد حملات از تعداد آسیب پذیری ها بیشتر می باشد، زیرا می توان از یک آسیب پذیری به دفعات متوالی حمله به سیستم های کامپیوتری انجام داد.



شکل ۲-۱ تعداد حملات گزارش شده بر حسب سال توسط CERT/CC

¹ Vulnerability

یکی از دلایل افزایش روزافزون مشکلات امنیتی در سیستم های کامپیوتری، به علت مکانیزم ساخت نرم افزار و محیطی که نرم افزار در آن اجرا می شود، است. امروزه نرم افزارها از اجزاء مختلف تولید شده توسط سازندگان گوناگون، ساخته می شوند. بنابراین امنیت درونی این اجزاء به تنهایی برای امنیت سیستم نرم افزار کافی نیست. بلکه باید ارتباطات بین این اجزاء و نحوه چینش آنها در کنار یکدیگر به گونه ای باشد که برای امنیت سیستم، مشکلی ایجاد نکند. همچنین نرم افزارهای امروزی، معمولاً در سیستم های مبتنی بر شبکه و توزیع شده استقرار می یابند. این گونه سیستم ها با اتصال به شبکه اینترنت در دسترس حملات گوناگون از سوی رخنه گران در سرتاسر دنیا قرار خواهند داشت. بنابراین باید مکانیزم هایی اتخاذ نمود که سیستم های نرم افزاری توزیع شده از تهدیدهای افراد ناشناس مصون بمانند.

مطالعات کلاسیک انجام شده درباره امنیت سیستم های کامپیوتری بر روی چگونگی اطمینان از محرمانگی، یکپارچگی و در دسترس بودن سیستم های کامپیوتری متمرکز است [۳]. و در این زمینه معمولاً به تولید پروتکل های ارتباطی امن، رمزنگاری و به کار بردن مکانیزم های امنیتی خارجی پس از تولید نرم افزار توجه شده است. با وجود مطالعات زیاد انجام شده در امنیت، توجه بسیار کمی به نحوه ساخت و مهندسی امنیت در نرم افزار شده است و این امر، با توجه به گسترش ساخت نرم افزار با استفاده از اجزاء گوناگون و نیاز به یک روش مهندسی در ایجاد ارتباط و قرار دادن اجزاء کنار هم، از اهمیت زیادی برخوردار گشته است، به گونه ای که با وجود حملات اندک بر روی روش های رمزنگاری [۴]، عمده حملات انجام شده بر روی سیستم های نرم افزاری، به علت طراحی ضعیف و غلط نرم افزار بوده است. به همین علت برای جلوگیری از گسترش روزافزون حملات باید علاوه بر تولید یک سیستم امن از دیدگاه رمزنگاری، به جنبه مهندسی نرم افزار آن نیز توجه داشت.

با توجه به مسائل مطرح شده در فوق، امنیت، همچون نیازهای کیفی دیگر باید در معماری نرم افزار مورد توجه قرار گرفته و مدل شود. برای مشخص شدن اهمیت معماری نرم افزار در تولید سیستم های امن، می توان به وب سرور معروف شرکت مایکروسافت به نام IIS^۱ اشاره کرد. این وب سرور دارای مشکلات متعدد امنیتی بود و استفاده از آن روز به روز کاهش می یافت. با این وجود، مایکروسافت پس از طراحی مجدد معماری نرم افزار این وب سرور و بدون معرفی تکنیک های جدید رمزنگاری، تحول چشمگیری در امنیت این وب سرور ایجاد نمود و مجدداً آن را به یکی از وب سرورهای محبوب دنیا تبدیل نمود [۵]. نرم افزار IIS، در سال ۱۹۹۵ توسط شرکت مایکروسافت برای ویندوز ۹۵ معرفی و در

¹ Internet Information Service

طی سال ۹۵ تا ۲۰۰۱ نسخه های مختلفی از آن ارائه گردید که نسخه ۵ آن در سال ۲۰۰۱ ارائه شد. ولی در طول این سالها همواره دارای آسیب پذیری های فراوان امنیتی بود که برخی از این آسیب پذیری ها موجب خطرات جدی امنیتی گشته و خسارات زیادی را به بار آورد. در سال ۲۰۰۳، شرکت مایکروسافت تصمیم گرفت که در نسخه ۶ این نرم افزار تغییرات عمده معماری را به وجود آورد. و به علت تغییرات به وجود آمده، رشد چشمگیری در امنیت این نرم افزار ایجاد گردید.

۲-۱ رویکرد حل مسئله

در این پایان نامه، برای چگونگی تعریف مسئله، ارائه راه حل و ارزیابی آن، از چارچوب ISLab که در پیوست ۱ ارائه شده، استفاده می شود. ولی به طور کلی، برای حل مسئله مدلسازی ویژگی های کیفی در سطح معماری نرم افزار، ابتدا مراحل انجام مدلسازی ویژگی های کیفی مشخص شده و زبان مدلسازی به عنوان یکی از نیازهای اصلی مدلسازی ویژگی های کیفی معرفی شده است. سپس مسئله مدلسازی ویژگی های کیفی، برای ویژگی کیفی امنیت و تاکتیک مدیریت اعتماد آن حل شده است. برای این منظور زبان UML برای مدلسازی انتخاب شده و با توجه به کمبود های UML در مدلسازی مفاهیم پایه مدیریت اعتماد، این زبان برای پوشش مفاهیم مورد نظر گسترش داده شده است. در ادامه بر اساس زبان گسترش داده شده، تعدادی الگوی معماری برای مدلسازی تاکتیک مدیریت اعتماد ارائه گردیده است. سپس زبان گسترش یافته ارائه شده، برای مدلسازی ویژگی کیفی امنیت در یک سیستم مطالعه موردی مورد استفاده قرار گرفته و نشان داده شده است که زبان مورد نظر توانایی مدلسازی امنیت و ارزیابی آن را دارا است. همچنین زبان گسترش یافته، با تعدادی پارامتر ارزیابی برای یک زبان مدلسازی، ارزیابی شده و نقاط قوت و ضعف آن در مقایسه با چندین زبان مدلسازی دیگر بررسی شده است.

۳-۱ مهمترین دستاوردهای پروژه

مهمترین دستاوردها و نوآوری های پروژه به صورت زیر می باشد:

- ۱- ارائه چارچوب ISLab برای پژوهش در حوزه نرم افزار که حاصل ۱۵ سال تجربه پژوهش در حوزه مهندسی نرم افزار در آزمایشگاه سیستم های هوشمند دانشگاه امیرکبیر بوده و در این پایان نامه این تجارب در قالب یک چارچوب مشخص به همراه فرایند، روش، راهنمایی و ابزارهای مربوط به آن ارائه شده و طریقه استفاده از چارچوب به طور عملی برای ایجاد روشی نو برای مدلسازی ویژگی های کیفی در معماری نرم افزار نشان داده شده است.

- ۲- ارائه چارچوبی برای مقایسه کارهای انجام شده در زمینه مدلسازی کنترل دسترسی و مدیریت اعتماد و مقایسه کارهای انجام شده در این زمینه. این چارچوب برای افرادی که قصد پژوهش در زمینه مدلسازی کنترل دسترسی یا مدیریت اعتماد را دارند سودمند بوده و نقاطی که می-توان در آنها به انجام پژوهش پرداخت را مشخص می کند.
- ۳- ارائه زبان UMLTrust، که زبانی گسترش یافته، مبتنی بر UML، با توانایی مدلسازی کنترل دسترسی و مدیریت اعتماد در سطح معماری نرم افزار است. مدل های ایجاد شده توسط این زبان می تواند برای طراحی، مستند سازی و ارزیابی معماری نرم افزار سیستم های امن مورد استفاده قرار گیرد.
- ۴- ارائه چارچوبی برای ارزیابی زبان های مدلسازی که این چارچوب با ارائه تعدادی پارامتر ارزیابی، امکان مقایسه مبتنی بر ویژگی را برای چندین زبان مدلسازی فراهم نموده و می توان به کمک آن نقاط قوت و ضعف هر روش را تعیین نمود.

۱-۴ ساختار پایان نامه

در ادامه، ساختار پایان نامه ارائه خواهد شد. در فصل ۲، مفهوم ویژگی های کیفی و روش و نیاز-مندی های مدلسازی آن در معماری نرم افزار معرفی شده است. در فصل ۳، مفاهیم پایه در زمینه امنیت معرفی شده و جایگاه کار انجام شده در امنیت و معماری مشخص خواهد شد. سپس مفهوم مهندسی نرم افزار سیستم های امن معرفی شده و جایگاه کار انجام شده در مهندسی نرم افزار سیستم های امن مشخص می شود. سپس به بررسی کارهای انجام شده در حوزه مسئله، یعنی مدلسازی کنترل دسترسی و مدیریت اعتماد در سطح معماری پرداخته خواهد شد. در فصل ۴، چارچوب RT به عنوان چارچوب و زبانی مجرد برای برآورده کردن نیازهای مدلسازی مدیریت اعتماد معرفی شده و نقاط ضعف آن مشخص می شود. سپس استفاده از UML برای پوشش نقاط ضعف مورد نظر پیشنهاد شده و روش های گسترش این زبان برای برآورده نمودن نیازهای مدلسازی بررسی می شود. سپس یکی از روش های گسترش انتخاب شده و زبان UMLTrust برای برآورده نمودن نیازهای مدلسازی ارائه خواهد شد و به همراه آن تعدادی الگوی معماری معرفی می گردد. در فصل ۵، یک سیستم نمونه با استفاده از زبان UMLTrust مدل شده و توانایی زبان در مدلسازی مدیریت اعتماد مشخص خواهد شد. در فصل ۶، زبان UMLTrust به وسیله تعدادی پارامتر ارزیابی خواهد شد. در فصل ۷ خلاصه و نتیجه گیری ارائه شده و پیشنهاداتی برای کارهای آینده ارائه می شود. در انتها نیز مراجع مورد استفاده در این کار معرفی می گردد.

فصل ۲ ویژگی‌های کیفی در معماری نرم افزار

۱-۲ مقدمه

برای مشخص شدن تعریف ویژگی‌های کیفی، ابتدا باید نیازهای کارکردی و غیرکارکردی را تعریف کنیم. نیازهای کارکردی، نیازهایی از سیستم هستند که مستقیماً متوجه یک کارکرد، فعالیت و یا رفتار از سیستم باشند. نیازهای غیرکارکردی، محدودیت‌ها و قوانینی بر روی ویژگی‌های مختلف نیازهای کارکردی سیستم می‌باشند [۶].

با توجه به تعریف ارائه شده در فوق، ویژگی‌های کیفی، نیازهایی از سیستم هستند که جنبه غیر کارکردی دارند. این نیازها در مراحل طراحی، پیاده سازی و استقرار سیستم باید مد نظر قرار گیرند [۱]. باید توجه داشت که برآورده ساختن یک نیاز کیفی، بر روی دیگر نیازهای کیفی اثرگذار است. به عنوان مثال، سیستمی که دارای ویژگی کیفی امنیت می‌باشد، معمولاً دارای ویژگی قابلیت اطمینان نیز است. یا برای مثال سیستمی که دارای کارایی مناسبی می‌باشد، قابلیت تغییر پایین‌تری می‌باشد. در [۷] ارتباط بین ویژگی‌های کیفی گوناگون بیان شده است.

برآورده کردن ویژگی‌های کیفی، مستلزم توجه به آنها در همه مراحل تولید سیستم، شامل معماری، طراحی، پیاده سازی و استقرار است. اولین مرحله‌ای که در آن به ویژگی‌های کیفی توجه شده و ویژگی‌های کیفی در آن مورد ارزیابی قرار می‌گیرند، مرحله تولید معماری نرم‌افزار سیستم است. بنابراین ویژگی‌های کیفی باید در معماری نرم‌افزار مورد توجه قرار گرفته و برای اینکه امکان مستند سازی و ارزیابی آنها در معماری نرم‌افزار فراهم گردد، مدل شوند.

با توجه به ارتباط ویژگی‌های کیفی با معماری نرم‌افزار در بخش بعدی معماری نرم‌افزار را تعریف کرده و سپس چگونگی تعیین نیازهای کیفی و سپس دستیابی به آنها را در سطح معماری نرم‌افزار نشان خواهیم داد.

۲-۲ معماری نرم افزار

برای معماری نرم‌افزار، تعریفی که به طور عمومی پذیرفته شده باشد، وجود ندارد. افراد مختلف، معماری نرم‌افزار را به اشکال گوناگون تعریف کرده‌اند. این تعاریف، از لحاظ ظاهری متفاوتند، ولی به مفهوم مشترکی اشاره می‌کنند .

در [۱] معماری نرم‌افزار به صورت زیر تعریف شده است :