تاریخ دریافت مقاله: ۱۳۹۰/۹/۲۱
تاریخ پذیرش مقاله: ۱۳۹۰/۱۲/۶

فصلنامه علوم و فنون نظامی، سال هفتم،
شماره۱۹، زمستان ۱۳۸۹
صص: ۳۷-۲۵

لزوم چارچوب امنیتی برای زیرساخت نرم‌افزاری مبتنی بر معماری سرویس‌گرا گرید (Grid SOA)

میرعلی سیدی[۱]
شهاب بهجتی[۲]
حمیدرضا افشارراد[۳]

چکیده :

در میان پیچیدگی شبکه فراگیر خدمات (GI&SG)، مسائل زیادی در حوزه امنیت نمایان می‌شود که عملکرد فعلی امنیت گرید نمی‌تواند نیازهای آن شبکه را تامین نماید. در نتیجه، مطالعه مسائل امنیتی شبکه مذکور را مهم، پیچیده و دشوار می‌سازد. در این تحقیق، ما جهت پوشش دادن نیازمندی‌های امنیتی شبکه فراگیر خدمات چارچوبی برای معماری امنیت ارائه کرده و مزایای آن را توضیح داده‌ایم. چارچوب ارائه شده برمبنای مدل مرجع معماری باز سرویس گرید بوده و دارای ۲ بخش اصلی می‌باشد: مدیریت جامعیت امنیت و پیاده‌سازی سیاست امنیتی.

مدیریت امنیت رویدادها، سیاست امنیتی، تضمین نرم‌افزار، سامانه و سرویس، اعمال قواعد امنیتی، مدیریت چرخه حیات دسترسی و شناسه، مدیریت تهدید و آسیب‌پذیری، الگوریتم‌های امنیتی، امنیت داده، زیرساخت گواهی، نظارت، و جامعیت امنیت از جمله خصوصیات کلان چارچوب معماری امنیت شبکه فراگیر خدمات به شمار می‌روند.

عدم وجود چارچوبی که به طور کامل با نیازهای مشخص شده در طرح جامع فاوا منطبق باشد، سبب توجه به موضوع و بررسی آن در این مقاله شده است.

کلید واژگان:

چارچوب امنیت، شبکه فراگیر خدمات، معماری سرویس‌گرا (S.O.A)، سرویس‌های توزیع شده، فناوری گرید.

---

[۱]- استادیار دانشگاه آزاد اسلامی واحد تهران مرکز

[۲]– عضو هیات علمی دانشگاه صنعتی مالک اشتر

[۳]- کارشناسی ارشد کامپیوتر گرایش نرم‌افزار(عهده‌دار مکاتبات)

مقدمه

تنوع درخواست‌ها، کثرت خدمات مورد نیاز، تعدد کاربران، گستردگی نرم‌افزارها، نیاز به سرعت زیاد در پاسخگویی سامانه‌ها، ما را به سمت استفاده از شبکه‌های مبتنی بر معماری گرید به منظور ایجاد یک شبکه فراگیر در سازمان سوق می‌دهد که به شبکه فراگیر خدمات[۱] (GI&SG) معروف است. در تدوین زیرساخت نرم‌افزاری برای این شبکه فراگیر خدمات، از معماری مرجع سرویس‌گرا[۲] و معماری مرجع گرید استفاده شده است.

شبکه فراگیر خدمات یک محیط توزیع شده[۳] یکپارچه می‌باشد که در آن، خدمات با هم در تعامل می‌باشند. اطمینان از جامعیت[۴]، محرمانگی[۵] و امنیت سرویس‌ها[۶] از طریق یک مدل مفهومی یا چارچوب امنیت، یک مولفه حیاتی به شمار می‌رود. ضمن در نظر گرفتن همه توانمندی‌های امنیت در سامانه، نیاز است که در امنیت شبکه فراگیر خدمات، چالش‌های کلیدی مربوط به حوزه‌های امنیت به صورت توزیع شده و چگونگی انجام تعامل بین اجزای سامانه نیز در نظر گرفته شود.

آنچه سبب اعتماد به شبکه فراگیر خدمات خواهد شد، وجود یک چارچوب امنیتی مناسب و منطبق با خصوصیات و وظایف سامانه است. در تدوین چارچوب امنیتی ذکر شده، به مفاد استانداردها و مدل های مختلف حوزه امنیت از جمله معماری باز سرویس‌گرید[۷] (OGSA) توجه شده است.

ادبیات تحقیق

از آنجایی که رویکرد فرماندهی و کنترل در تدوین طرح جامع فاوا وجود دارد، ضروری است فرمانده به عنوان درخواست‌کننده خدمات بتواند سرویس‌های مورد نیاز خود را به صورت امن و با رعایت حیطه‌بندی و طبقه‌بندی از شبکه فراگیر خدمات دریافت نموده و از وضعیت زیرمجموعه‌اش در هر زمان و مکان، به طور کامل آگاهی پیدا کند و در صورت لزوم دستورات لازم را به آنها ابلاغ نماید. بنابراین سامانه باید بتواند درخواست‌های ورودی را به

1- Global Information & Service Grid
2- Service Oriented Architecture (SOA)
3 -Distributed
4 -Integrity
5- Confidentiality
6 -Security of the Services
7- Open Grid Service Architecture (OGSA)

طور کامل و به درستی از کاربر دریافت نموده و بعد از بررسی و احراز هویت کاربر و براساس میزان دسترسی‌های او به منابع موجود در سامانه، درخواست او را پردازش و نتیجه را به شکل گزارش یا هر قالب دیگری که در سامانه دیده شده، به وی ارائه نماید.

سابقه گرید مربوط به سال ۱۹۶۹ پس از جنگ جهانی دوم می‌باشد که با به هم پیوستن شبکه‌های بزرگ و کوچک در سراسر جهان اینترنت پا به عرصه ظهور نهاد. در شبکه اینترنت از مزیت به اشتراک گذاشته شدن منابع، مثل رسانه‌های ذخیره‌ساز، استفاده می‌شود و از توان محاسباتی هیچ بهره‌برداری نمی‌شود. به اشتراک گذاشته شدن پردازنده‌ها در گرید ایده‌ای است که نیاز به آن کاملا محسوس می‌باشد. این موضوع مقدمه‌ای برای ظهور خوشه‌ها[1] شد. که مجموعه‌ای از رایانه‌های همگن متصل به هم است که برای اجرای یک برنامه طبق اسلوب مشخص با یکدیگر در ارتباط می‌باشند. خوشه‌ها به علت اتصال قوی و مطمئن میان آن‌ها می‌توانند کارهای سنگین محاسباتی را در زمان کوتاهی انجام دهند. با این حال کاربرد خوشه ها در اغلب مواقع با مشکلاتی به همراه است. برخی از محدودیت‌های محیط خوشه که می تواند کاربر را با چالش مواجه سازد، عبارت‌اند از :

۱) منابع را به‌صورت اختصاصی در اختیار می‌گیرند و این مسئله مانع تشکیل خوشه‌های بزرگ برای انجام کارهای محاسباتی بزرگ می‌شود.
۲) هزینه تشکیل یک خوشه برای یک شرکت شاید مقرون به صرفه نباشد. بنابراین اغلب ترجیح می‌دهند خوشه‌های موجود را برای مدت اجرای برنامه خود اجاره کنند تا هزینه‌ها بخصوص هزینه‌های نگهداری کمتر شود
۳) از آنجایی که قدرت اقتصادی هر موسسه‌ای در جهان محدود است. به دنبال ابداع شیوه‌های بسیار کاراتر و کم‌هزینه‌تری هستند بنابراین دیگر تشکیل خوشه‌های بزرگ مزیت اقتصادی سابق را ندارد. (کاشانی، ۱۳۸۸، ص۹)

معماری گرید و معماری سرویس‌گرا ما را به سمت مبحث رایانش ابری[2] سوق می‌دهد. در رایانش ابری، به همه خدماتی که به کاربران ارائه می‌گردد، به عنوان سرویس نگاه می‌شود. به عنوان مثال می‌توان به موارد زیر اشاره کرد:

---

[1]- Clusters
[2]- Cloud Computing

منبع ذخیره‌سازی به شکل سرویس[۱]، پایگاه داده به‌شکل سرویس[۲]، ارائه اطلاعات در قالب سرویس[۳]، ارائه فرآیند به‌صورت سرویس[۴]، برنامه‌های کاربردی به شکل سرویس[۵]، ارائه‌ی سکو به‌صورت سرویس[۶]، امکان یکپارچه‌سازی به‌صورت سرویس[۷]، امکان ایجاد امنیت به‌شکل سرویس[۸]، فراهم نمودن امکان مدیریت/نظارت به‌شکل سرویس[۹]، امکان تست به‌صورت سرویس[۱۰]، ارائه زیرساخت به‌صورت سرویس[۱۱] (ایزایران، ۱۳۸۹، ص۱۲۱).

تحلیل محتوا

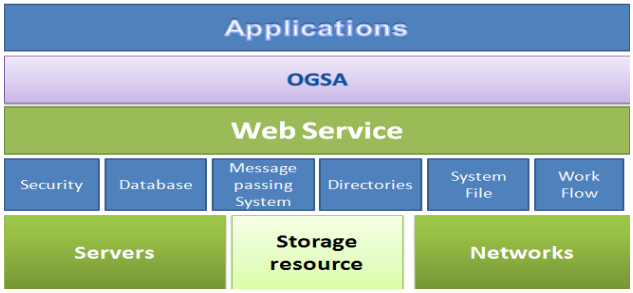
هدف اصلی شبکه فراگیر خدمات فراهم کردن سرویس‌هایی است که یک کامپیوتر به تنهایی قادر به ارائه آن سرویس‌ها نمی‌باشد. این کار از طریق به هم پیوستن منابع مختلف به صورت پویا و ایجاد سرویس‌های جدیدی فراهم می آید. شبکه فراگیر خدمات، کاربرها، برنامه‌های کاربردی و منابع را قادر می سازد تا به صورت بلادرنگ[۱۲] از طریق یک فضای کاری مجازی[۱۳] با همدیگر محاوره و تعامل داشته باشند.

بررسی‌های انجام شده در سال‌های اخیر نشان می‌دهد، بین اهداف گرید و سودمندی‌های معماری سرویس‌گرا که بر روی سرویس‌های وب بنا شده است، ارتباط و هم‌پوشانی وجود دارد. سرعت پیشرفت در فناوری‌ها و استانداردهای وب‌سرویس‌ها، یک مسیر جدید در امتداد معماری گرید سرویس‌گرا فراهم کرده است. همگرایی بین معماری سرویس‌گرا (SOA) و گرید، در معماری باز سرویس گرید[۱۴] ارائه شده توسط گروه جهانی گرید[۱۵] (GGF) در نظر

---

[1]- Storage as a Service
[2]- Database as a Service
[3] Information as a Service
[4] Process as a Service
[5] Application as a Service
[6] Platform as a Service
[7] Integration as a Service
[8] Security as a Service
[9] Management/governance as a Service
[10] Testing as a Service
[11] Infrastructure as a Service
[12] Real Time
[13] Virtual workspace
[14] Open Grid Service Architecture (OGSA)
[15] Global Grid Forum

گرفته‌شده‌است. گروه جهانی‌گرید با ارائه معماری باز سرویس‌گرید و جمع‌آوری استانداردهای باز، مانند زبان تعریف سرویس‌های وب[۱] توانسته است استانداردی آسان و در عین حال دقیق برای سامانه‌های گرید تعریف کند. از آن گذشته، معماری باز سرویس گرید (OGSA) از تجربیات بدست آمده از پروژه‌های بزرگی مانند گلوباس نیز بهره‌مند است. شکل زیر، ساختار معماری این استاندارد را نشان می‌دهد .



شکل ۱ : ساختار معماری باز سرویس‌های گرید

استانداردهای باز و پروتکل‌های این معماری راه تولید سرویس‌ها را نشان می‌دهند. این سرویس‌ها قلب گرید هستند و در واقع به استفاده‌کننده اجازه می‌دهند با گرید کار کند.

جنبه‌های امنیتی و مهم در سامانه‌های مبتنی بر معماری گرید شامل احراز هویت، اجازه نمایندگی و وکالت[۲]، مجوز کوتاه‌مدت[۳]، مجوز دسترسی[۴]، مجوز اجرای سیاست‌های سیاست‌های پنهان[۵]، محرمانه‌گی[۶]، جامعیت داده/اطلاعات/پیام[۷]، برقراری سیاست امنیتی[۸] و جنبه‌های امنیتی معماری سرویس‌گرا شامل تعیین هویت، اعتبارسنجی، نقطه ورود مشترک، رازداری، جامعیت، امنیت سطح انتقال، امنیت سطح پیام، رمزگذاری و

---

[1] -Web Services Description Language

۲- (Delegation به معنی تهیه مکانیزم‌هایی جهت اجازه نمایندگی برای دستیابی صحیح

۳-(Single Logon) به معنی تغییر دادن یک مجوز برای یک بازه زمانی کوتاه

۴- (Authorization) به معنی توانایی کنترل دستیابی به اجزای گرید.

۵- (Privacy) به معنی دادن مجوز، هم به درخواست‌کننده سرویس

۶ - (Confidentiality) به معنی حفاظت از محتوای پیام‌ها و امور محرمانه می‌باشد.

۷- (Data/Information/Message Integrity) به معنی حصول اطمینان از کشف و تشخیص تغییرات غیر مجاز وارد شده در محتوای پیام‌ها یا داده‌ها است.

۸- (Policy Exchange) به معنی برقرار کننده مکانیزم‌های امنیتی است

امضاهای دیجیتالی، از مواردیست که در لایه های مختلف شبکه فراگیر خدمات براساس استاندارد مورد استفاده باید در نظر گرفته شود.

چارچوب امنیت و مطلوبیت نرم‌افزارهای کاربردی

بیشتر استانداردهای صنعتی معماری سرویس‌گرا، در بستر XML تعریف شده‌اند. در چند سال گذشته توصیفات بسیاری مبتنی بر XML برای پوشش جنبه‌های امنیتی معماری سرویس‌گرا به وجود آمدند، که بسیاری از آنها بخشی از توصیفات سرویس‌های وب[1] هستند. (دارا، ۱۳۸۸، ص۶۵)

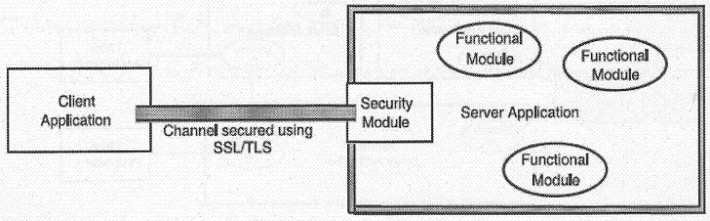
با پیشرفت فناوری و روش‌های طراحی سامانه‌های نرم افزاری انتظار می‌رود رویکردهای امنیتی جهت پیشگیری و مقابله با آسیب‌ها و نفوذها تغییر یابد. در خصوص سرویس‌گرایی نیز چنین است و رویکردهای سنتی امنیت، کارایی لازم را در معماری‌های سرویس‌گرا ندارند. برای درک بهتر لزوم به کارگیری رویکردی جدید در زمینه امنیت محیط‌های سرویس‌گرا بهتر است نگاهی دوباره به انگیزه استفاده از معماری‌های سرویس‌گرا بیندازیم.

برای رسیدن به اهداف اصلی معماری سرویس‌گرا، باید محدودیت‌های مربوط به افزایش چابکی و انعطاف‌پذیری سازمان‌ها، برطرف شود. به‌علاوه در محیط‌های غیر سرویس‌گرا، تفاوت‌های میان سکوها[2]، زبان‌های برنامه‌نویسی و پروتکل‌ها منجر به تشکیل مرزهای فناوری شده که عبور از آن‌ها مشکل است. به همین ترتیب در چنین محیط‌هایی فناوری‌های امنیتی نیز بیش از حد به مرزهای سازمانی تکیه کرده‌اند و موانعی را برای همکاری بین سازمانی به وجود آورده‌اند.

نکته مهم و قابل توجه این است که رویکردهای امنیتی سنتی با فرض وجود موانع مذکور، از آنها بهره می‌برند. به عنوان مثال طبق شکل (۲)، کاربرد سرویس‌دهنده[3]، ضمن مدیریت امنیت مربوط به خود، برای حفاظت داده‌هایی که با کاربردهای سرویس‌گیرنده[4] مبادله می‌کند، بر کانال‌های انتقال امن تکیه می‌کند.

---

[1] Web Service specifications (WS-*)
[2] Platforms
[3] Server Application
[4] Client Applications

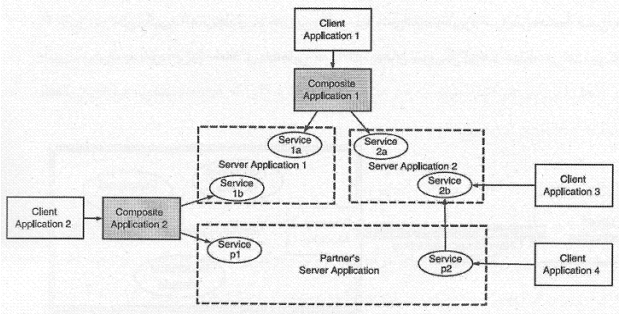


شکل ۲ : معماری امنیت کاربرد سنتی(لاله پرور، ۱۳۸۹، ص۴۰)

هرچند چنین تصویری از نحوه‌ی تأمین امنیت برای محیط‌های کاربرد محور به خوبی عمل می‌کند، اما به دلیل وجود دو فرض ضمنی زیر نمی‌تواند راه‌حلی مناسب در سیستم‌های سرویس‌گرا باشد:

- کاربرد سرویس‌دهنده از مدل امنیتی مناسب مطلع است. منظور از مدل امنیتی این است که چه کسی در رابطه با امنیت تصمیم‌گیری می‌کند و این امر در چه زمان و به چه صورتی انجام می‌شود.
- کاربرد سرویس‌دهنده به‌اندازه‌ای مورد اعتماد است که بتواند تمام داده‌ها را- شامل هر داده‌ی حساسی که سرویس‌گیرنده می‌فرستد- مشاهده نماید.

همان‌طور که در تصویر محیط سرویس‌گرای (شکل۳) دیده می‌شود از ترکیب سرویس-هایی که چند کاربرد مختلف - حتی کاربردهایی که به سازمان دیگری تعلق دارند- ارائه کرده‌اند، می‌توان کاربردی مرکب ایجاد کرد. همچنین سرویس‌های یک سازمان می‌توانند به‌صورت مستقیم یا به وسیله کاربردهای سازمان‌های شریک فراخوانده شوند.



شکل ۳ : ارتباط کاربردهای سرویس دهنده و سرویس گیرنده در سامانه های سرویس‌گرا(لاله پرور، ۱۳۸۹، ص۴۱)

واضح است که در چنین ساختاری، پیش‌بینی تمام وضعیت‌های ممکن در زمینه فراخوانی یک سرویس برای طراح سامانه مشکل است. بنابراین کاربردها دیگر نمی‌توانند مسئولیت اعمال امنیت را برعهده بگیرند. به عبارت دیگر، مدل‌های امنیتی را نمی‌توان به صورت صریح در کد تک‌تک کاربردها قرار داد. همچنین با توجه به این که یک بخشی یا تمام یک پیام مربوط به کاربردی خاص از سازمان می‌تواند به کاربردهای دیگری ختم شود، باید امکان دسترسی هر یک از کاربردها به داده‌های مورد نیازشان را به شکل صحیحی محدود کرد. از آنجایی که مرزهای میان سازمان‌ها و کاربردها، همانند گذشته مانعی برای استفاده مجدد از منابع (در اینجا سرویس‌ها) به وجود نمی‌آورند، استفاده از رویکردهای سنتی برای امنیت این گونه محیط‌ها کفایت نمی‌کند.

جهت تکمیل بحث، اشاره‌ای به بررسی تحقیقاتی آقای راماچاندران[1] که در سال ۲۰۰۲ در خصوص امنیت در توسعه نرم‌افزارها انجام دادهاست؛ می‌شود. ایشان ۴ مولفه زیر را برای توسعه نرم‌افزار ارائه نموده‌اند :

- خطاهای قابل کشف و دیگر ضعف‌های آن توسط توسعه‌دهندگان برطرف شوند.
- احتمال آنکه توسعه‌دهندگان بدخواه بتوانند خطاهای قابل کشف را در نرم‌افزار تعبیه کنند، کاهش داده شده یا به صفر برسد.
- نرم‌افزار باید حمله-پایدار[2]، حمله- تحمل‌پذیر[3] و یا حمله-انعطاف‌پذیر[4] باشد.
- تعاملات بین مولفه‌های نرم‌افزاری سیستم و بین سیستم و موجودیت‌های خارجی منجر به ضعف‌های قابل کشف نرم‌افزار نخواهد شد. (دارا، ۱۳۸۸، ص۲۹).

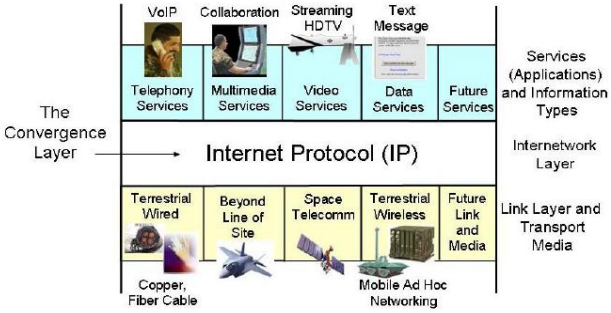
اثر چارچوب امنیت در زیرساخت ارتباطی

همانگونه که اشاره شد در شبکه فراگیر خدمات همه چیز به صورت سرویس به کاربران ارائه می‌شود و زیرساخت ارتباطی نیز یکی از این سرویس‌ها محسوب می‌شود. لایه زیرساخت معمولا از دو بخش انتقال اطلاعات و مدیریت شبکه ارتباطی تشکیل می‌گردد. امکانات در نظر گرفته شده در این لایه موجب مدیریت و برقراری ارتباطی فراگیر بین تمامی

---

[1] Ramachandaran
[2] Attack-Resistant
[3] Attack-Tolerant
[4] Attack-Resilient

بخش‌های نظامی از بالاترین رده تا پایین‌ترین رده ستادی و عملیاتی، می‌گردد. اهمیت حضور مولفه‌های چارچوب امنیتی در لایه زیرساخت با توجه به شکل زیر به وضوح نمایان است. عدم عملکرد به موقع مولفه امنیتی سبب نشت اطلاعات در لایه ارتباطات خواهد شد.



شکل ۴ : شمای کلی سرویس زیرساخت ارتباطی

با توجه به این که اطلاعات یکی از سرمایه‌های مهم سازمان‌ها از جمله سازمان‌های نظامی به شمار می‌آید، باید لایه‌های امنیتی سامانه، ضمن تضمین طبقه‌بندی اطلاعات، حیطه‌بندی اطلاعات را برای سایر کاربران سامانه در نظر بگیرند.

اثر چارچوب امنیت در تضمین اطلاعات

در شبکه فراگیر اطلاعات و خدمات، گروه‌های مختلف مشغول دریافت سرویس‌های اطلاعاتی و داده‌ای هستند. اطلاعات و وداده‌ها سرمایه‌های اصلی سازمان به شمار می‌آیند لذا حفاظت از اطلاعات یکی از وظایف اصلی چارچوب امنیتی برای صیانت از دارایی‌های سازمان محسوب می‌گردد. برای این کار می‌توان از ایجاد کنترل های امنیتی با سطح اطمینان متغیر در مبادی خروجی شبکه جهت کنترل تعاملات استفاده کرد. یکی دیگر از اثربخشی‌های مهم چارچوب امنیتی، نظارت، تشخیص، جستجو، ردیابی و پاسخ دائم به فعالیت‌های کارمندان داخلی و سوء استفاده‌های آنان می‌باشد.

با شناخت مولفه‌های مختلف چارچوب امنیتی برای شبکه فراگیر خدمات و استفاده صحیح از آنها، امکان مخدوش شدن اطلاعات، کاهش یافته و گامی در جهت ارتقای امنیت داده‌ها و اطلاعات شبکه فوق، برداشته می‌شود.

چارچوب امنیت و چگونگی پردازش امن درخواست های کاربران

همان‌طور که اشاره شد، سرویس گرید شبکه‌ای است شامل تعدادی زیادی ارائه کننده سرویس که همانند یک ابر تمامی سرویس‌ها را در برگرفته است. موضوع این است که مشتریان و کاربران قرار است به طور مستقیم با گرید ارتباط برقرار کنند و نه با سرویس‌ها. اصولا چون با گریدی از سرویس‌ها مواجه هستیم، طبق تئوری گرید باید یک میان‌افزار[۱] داشته باشیم تا عمل مجازی‌سازی[۲] بین استفاده‌کنندگان و گرید را انجام دهد. وظایفی مثل دریافت تقاضا[۳] از کاربر، قراردادن تقاضا در صف انتظار، پخش‌کردن[۴] تقاضا در گرید جهت اجرا، دریافت نتیجه اجرا و برقراری امنیت و ... در همه مراحل فوق، به عهده میان‌افزار می‌باشد. به دلیل این که تقاضادهندگان با میان‌افزار در ارتباط هستند، بنابراین هیچ اطلاعی از سرویس‌های موجود در گرید نخواهند داشت. هر سرویس دارای یک قلمرو امنیت مخصوص خود می‌باشد که باید به موقع ایفای نقش نماید. ۲ راه زیر برای اعمال امنیت در میان‌افزار گرید سرویس‌گرا به نظر می‌رسد:

الف) اعمال امنیت[۵] در میان‌افزار و یکپارچه بودن آن با مولفه امنیت در سرویس

در این حالت، میان‌افزار دارای یک مولفه امنیتی می‌باشد. هنگامی که تقاضایی از طرف یک درخواست کننده به میان‌افزار ارسال شود، مولفه امنیتی موجود در میان‌افزار که جنبه عمومی برای همه تقاضاها را دارد، فعال شده و بعد از انجام امور اولیه و عمومی امنیت، تقاضا توسط میان‌افزار به سرویس مورد نظر در گرید نگاشته می‌شود. سپس مولفه امنیتی سرویس فراخوانی شده اقدامات امنیتی خود را انجام می‌دهد. در این فرآیند بخش امنیتی میان‌افزار با بخش امنیتی سرویسی که تقاضای مشتری را اجرا می‌نماید، مرتبط شده[۶] و به صورت یکپارچه رویه امنیتی را برای متقاضی اجرا می‌کنند.

ب) اعمال امنیت سرویس درخواست شده در میان‌افزار

در این حالت برخلاف روش بالا هیچ مولفه امنیتی در میان‌افزار وجود ندارد. هنگامی که درخواستی توسط کاربر به میان‌افزار می‌رسد، میان‌افزار با سرویس مورد نظر ارتباط برقرار

---

[1]- Middleware
[2]- Virtualization
[3]- Request
[4]- Dispatching
[5]- Public Security Policy
[6] -Integrated

کرده و مولفه امنیتی آن سرویس را جهت پاسخگویی به تقاضای وارده، فرامی‌خواند سپس درخواست کاربر از لحاظ امنیتی توسط مولفه امنیت سرویس مورد بررسی قرار می‌گیرد. در واقع در این حالت میان‌افزار مسیرگزینی[۱] امنیت را انجام می‌دهد.

در نهایت، بعد از مثبت بودن نتایج حوزه امنیت، سرویس فراخوان شده به متقاضی ارائه می‌گردد. پرداخت پول از طریق دستگاه‌های خودپرداز بانک در حالت شتاب و بدون شتاب نمونه‌ای از چنین سامانه‌هایی محسوب می‌شود. به عنوان یک مثال دیگر، سرویس‌گرید حسگرها[۲] را در نظر بگیرید، که به درخواست فرمانده جهت مطلع شدن از وضعیت منطقه (زمین، هوا، دریا) پاسخ می‌دهد. حسگر رادار، حسگر انسانی و... هر کدام با عملکرد یکسان ولی با سیاست امنیتی متفاوت بعد از احراز هویت نتیجه را به فرمانده ارسال می‌نماید. برای فرمانده به عنوان سرویس‌گیرنده همه چیز شفاف بوده و چگونگی اقدام حسگرها اهمیتی ندارد. آنچه اتفاق می‌افتد یکپارچگی و جامعیت مولفه‌های سامانه از جمله مولفه‌های امنیتی[۳] سرویس‌ها و میان‌افزار می‌باشد. در طرح جامع فاوا از ایده گرید اطلاعاتی فراگیر[۴] استفاده شده‌است. در این ایده، گرید به چندین خوشه افراز شده و به هر خوشه، سرویس گرید گفته می‌شود. در واقع یک ابر از خوشه‌ها به وجود آورده و برای هر حوزه کاری و ماموریتی یک خوشه در نظر گرفته می‌شود که تمامی تعاملات موجود شامل تعامل بین خوشه‌ها و تعامل کاربران با خوشه‌ها به صورت رویدادگرا[۵] و رویدادها نیز از نوع پیام[۶] انجام می‌شود.

نتیجه‌گیری

در هر یک از سرویس‌گریدهای داخل ابر سرویس‌ها، مثل سرویس گرید حسگر، سرویس گرید کنترل، سرویس گرید اقدام، سرویس گرید هوشمندی[۷] و سایر سرویس گریدها، سرویس‌هایی وجود دارند که همگی از یک جنس بوده و باید امنیت آنها در سامانه اعمال گردد. تحلیل درخواست کاربران، پیدا کردن گرید و نگاشت درخواست کاربر به سرویس مربوطه، تصدیق هویت کاربر، جامعیت داده‌ها، صحت تعاملات، کنترل دسترسی، ارائه پاسخ

---

[1]- Routing
[2]- Sensors
[3]- Security Policy Integration
[4] Global Information Grid (GIG)
[5] Event Driven
[6] Message
[7]- Intelligence

به صورت امن به درخواست کننده واقعی و... در لایه‌های مختلف سامانه از جمله وظایفی است که میان‌افزار امن باید انجام دهد.

برقراری موارد فوق، بدون وجود یک ساختار منظم که منطبق با معماری‌های به کار رفته در طراحی شبکه فراگیر خدمات باشد، امکان‌پذیر نیست. ضمن این که به دلیل تنوع خدمات، تعدد کاربران و گستردگی امور در طرح جامع فاوا، در چارچوب امنیتی فوق باید دیدگاه‌ها و جنبه‌های نظامی نیز در نظر گرفته شود تا بتوان نیازمندی‌های مختلف نظامی از جمله فرماندهی عملیات را پشتیبانی کرد.

وجود چارچوب فوق به تیم معماری فنی فناوری اطلاعات و ارتباطات کمک خواهد کرد تا محصولات تهیه شده براساس طرح جامع فاوا را با استفاده از ویژگی‌های چارچوب پیشنهادی بررسی و منطبق نمایند. همچنین، چارچوب فوق الگویی برای ارزیابی امنیت در سامانه‌های فناوری اطلاعات و ارتباطات آجا براساس طرح جامع فاوا برای متولیان حوزه امنیت خواهد بود و کمک می‌کند تا انطباق مفاد اسناد درخواست‌های پیشنهادیه[1] (RFP) پروژه‌ها، با سرعت و دقت بیشتری انجام شود.

بطور کلی می‌توان نتایج تحقیق را به صورت زیر دسته‌بندی نمود:

- امکان بررسی و انطباق ویژگی‌های وظیفه‌مندی و غیر وظیفه‌مندی امنیت در مفاد اسناد درخواست پیشنهادیه پروژه‌های طرح جامع فاوا.
- دستیابی به الگو و چارچوبی برای طرح ریزی، خط و مشی دهی، برنامه ریزی، هدایت، نظارت و کنترل نقشه راه طرح جامع فاوا.
- تهیه مستنداتی جهت بهره برداری سایر متخصصین و نظریه پردازان فاوا.

[1]- Request For Proposal (RFP)

منابع:

۱. دارا، عمار، (۱۳۸۸)«ارائه یک مدل تلفیقی برای تضمین امنیت معماری سرویس‌گرا»، پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات.

۲. کاشانی، محسن، (۱۳۸۸) «ارائه یک معماری بهبود یافته سرویس‌گرا مبتنی بر گرید»، پایان نامه کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار، دانشگاه آزاد اسلامی، واحد نجف‌آباد.

۳. جورج سادوسکای...[ودیگران]،(۱۳۸۴) گروه مترجمین: مهدی میردامادی، زهرا شجاعی، محمدجواد صمدی، راهنمای امنیت فناوری اطلاعات، دبیرخانه شورای عالی اطلاع‌رسانی، تهران.

۴. فتح‌اللهی، علی(۱۳۸۳) «بررسیUML از نظر قابلیت پوشش به چارچوب زکمن»، پایان‌نامه کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار، دانشگاه شهید بهشتی.

۵. لاله پرور، (۱۳۸۹) «رویکردهایی جهت کاهش خطرات امنیتی در سیستم های مبتنی بر معماری سرویس‌گرا»، پایان نامه کارشناسی ارشد مهندسی کامپیوتر- نرم‌افزار، دانشگاه آزاد اسلامی، واحد علوم تحقیقات.

۶. ایزایران، (۱۳۸۹) «معماری کلان زیرساخت نرم‌افزاری»، پیش‌نویس سند پروژه.

منابع انگلیسی

7. OASIS, Reference Architecture for Service Oriented Architecture Version 1.0 (2008).
8. Goertzel, Mercedese, K., [and others]: Software Security Assurance:State-Of-The-Art-Report (SOAR) (2007).
9. Ramachandaran, J. :Designing Security Architecture Solutions, John Wiley & Sons Inc (2002).
10. Kanneganti, R. , Chodavarapu, P. : SOA Security, Manning (2007).
11. ESD : Security – A major imperative for service-oriented Architecture.
12. Menzel,M., Wolter,C., Meinel,C.:Access Control for Cross Organisational Web Service Composition,Journal of Information Assurance and Security ,pp. 155-160 (2007).
13. Matzaj B. Jurikh, Ramesh Loganathan, Poornachandra Sarang, Frank Jennings, 2007, Packt Publishing " SOA Approach To Integration - XML, Web Services, ESB, And BPEL In real-world SOA Projects", PACKT Publishing.
14. P.Kanneganti, P.Chodavarapu, SOA Security, Manning Publications Co., ISBN:1-932394-680, 2007.