ششمین کنفرانس بین المللی انجمن رمز ایران
۱۵ و ۱۶ مهر ماه ۱۳۸۸، دانشگاه اصفهان
انجمن رمز ایران
دانشگاه اصفهان

معماری یک سیستم تشخیص نفوذ توزیع شده برای سرویسهای وب با رهیافت تشخیص ناهنجاری و بدرفتاری

میثم صفرعلی‌نجار[1]، محمد عبداللهی ازگمی[2]

گروه فناوری اطلاعات و ارتباطات، مرکز آموزش الکترونیکی، دانشگاه علم و صنعت ایران[1]
najjar@vc.iust.ac.ir
دانشکده مهندسی کامپیوتر، دانشگاه علم و صنعت ایران[2]
azgomi@iust.ac.ir

چکیده

در پیاده‌سازی معماری سرویس‌گرا، سرویس‌های وب نقش مهمی ایفا می‌کنند. امروزه توسعه برنامه‌های کاربردی تحت وب با استفاده از سرویس‌های وب شتاب بیشتری گرفته است. ولی در نقطه مقابل، امنیت موضوعی است که همیشه کاربرد سرویس‌های وب را به چالش کشانده است. در همین راستا با وجود استانداردهای امنیتی در حوزه سرویس‌های وب، در چند سال اخیر بکارگیری تجهیزات امنیتی حساس به XML رواج بیشتری یافته است. اما هنوز هم نفوذ از این معبر امکان‌پذیر است. ما در این نوشتار یک معماری سیستم تشخیص نفوذ برای سرویس‌های وب ارائه می‌کنیم و با ایده گرفتن از ساختار سیستم‌های تشخیص نفوذ رایج، معماری پیشنهادی از روش تشخیص بدرفتاری و ناهنجاری در ترافیک پیامهای SOAP استفاده می‌کند. درنتیجه، در برابر آسیب‌پذیری‌های ذاتی سرویس‌های وب، سطح دیگری از دفاع در کنار سایر تجهیزات امنیتی افزوده می‌شود. این معماری بصورت توزیع شده است، بنابراین قابلیت توسعه آن در سرویس‌های مختلف وبی که روی ماشین‌های مختلف در شبکه نصب هستند، وجود دارد.

واژه‌های کلیدی

سرویس‌های وب، سیستم تشخیص نفوذ، امنیت سرویس‌های وب، تشخیص ناهنجاری، تشخیص بدرفتاری

۱- مقدمه

سرویس‌های وب در اصل به‌عنوان پاسخی به نیاز یکپارچه‌سازی و همکاری سیستم‌های اطلاعاتی و انتقال اطلاعات بین آنها بوجود آمدند [1]. سرویس‌های وب بر پایه XML، SOAP، WSDL و UDDI استوارند. پروتکل SOAP[1] وظیفه انتقال اطلاعات مبتنی بر XML را به عهده دارد، WSDL[2] زبان توصیف سرویس وب و UDDI محل ذخیره و دسترسی عمومی مشخصات سرویس وب است [2، 3]. ویژگی استقلال از سکّو (سخت‌افزار، سیستم‌عامل و زبان برنامه-نویسی) دلیل مقبولیت عمومی سرویس‌های وب است. ولی متأسفانه مسئله امنیت نقطه تاریکی برای این فناوری است. سازمانهای توسعه دهنده وب مثل W3C و OASIS استانداردها و معیارهای مختلفی را برای این مسئله پیشنهاد می‌کنند؛ اما گذشته از قابلیت همکاری بین سرویس‌ها، بنا به سربارهایی که به سیستم اضافه می‌نمایند از استقبال عمومی چندانی برخوردار نیستند [4، 5].

سرویس‌های وب از پروتکل‌های لایه کاربرد، مثل HTTP برای انتقال درخواست‌ها و پاسخ‌ها بین سرویس‌دهنده و سرویس‌گیرنده استفاده می‌کنند. از اینرو، برای ارائه سرویس، درگاه‌های این پروتکل‌ها - مثل درگاه ۸۰ - نباید بسته باشد؛ این امر باعث می‌شود که معبری برای نفوذ مهاجمین به درون سازمانها گشوده شود. ابزارهای امنیتی رایج مثل دیوارهای‌آتش، فیلترهای محتوایی، سیستم‌های تشخیص و پیشگیری نفوذ قادر به تشخیص و سدّ حملاتی که از طریق سرویس‌های وب انجام می‌شود نیستند [6]؛ زیرا با کاستی‌هایی که این ابزارها در تشخیص حملات نهفته در متن پیامهای SOAP دارند، هرگز قادر به تشخیص خطرات پنهان در ترافیک ظاهراً قانونی شبکه نخواهند بود [7].

[1] Simple Object Access Protocol
[2] Web Service Definition Language

از طرفی در نظر گرفتن کلیه مسائل امنیتی برای توسعه‌دهندگان سرویس‌های وب، امری بسیار سخت و پیچیده است. همیشه این امکان وجود دارد که نفوذگران با صرف وقت کافی، پی به آسیب‌پذیری‌های سرویس برده و از این طریق حملات خود را طراحی نمایند. با وجود ابزارهای امنیتی حساس به XML و خاص سرویس‌های وب، قادر هستیم این نوع حملات را تشخیص و از آسیب‌های بیشتر پیشگیری نماییم.

انجام اموری روی ترافیک سرویس‌های وب که بر پایه اسناد XML است، مثل پیش‌پردازش، بررسی خوش‌شکلی اسناد، بررسی کارکترهای غیرمجاز، تجزیه[1] سند، وارسی سند با یک الگو[2] یا DTD و جلوگیری از حملات شناخته شده‌ای مثل تزریق SQL، تزریق XML، XSS، انواع حملات DoS و نظایر آن، بر عهده ابزارهایی مانند دیوارآتش‌های XML است [8، 9]. اما با وجود اقدامات امنیتی در سطوح مختلف، همه روزه شاهد آمارهایی مبنی بر وقوع حملات جدیدی از طریق اینترنت به درون سازمانها هستیم [12]. بنابراین می‌توان گفت که، این ابزارها قادرند حدی از امنیت را تأمین نمایند؛ لذا مکانیزم‌ها و فنون دیگری برای جبران کاستی‌ها نیاز است.

سیستم‌های تشخیص نفوذ، ابزارهایی هستند که در پاسخ به مسئله دور زدن سدّهای دفاعی، مثل دیوارآتش، کارآیی خوبی از خود نشان می‌دهند. این ابزار با القای مفهوم دفاع در عمق، ناظر ترافیک و رفتار عناصر شبکه است و درصورت عبور مهاجم از سطوح اول دفاع، قادر است با تولید هشدار یا پاسخ مناسب، مسئولین امنیتی سازمان را مطلع یا از ادامه حمله جلوگیری نماید [10]. عملکرد و مکان قرارگیری سیستم‌های تشخیص نفوذ در شبکه بسته به نوع آن متفاوت است. از لحاظ نوع روش تشخیص، این سیستم‌ها به دو دسته کلی مبتنی بر تشخیص بدرفتاری[3] و تشخیص ناهنجاری[4] تقسیم می‌شوند. در اولی الگوی حملات شناخته شده، اساس کار تشخیص است و در دومی نمایه‌های[5] رفتار عادی مؤلفه‌های شبکه. البته می‌توان دسته سومی نیز با روش تشخیص مبتنی بر مشخصه[6] اضافه نمود [10، 11]. همچنین، براساس محل جمع‌آوری اطلاعات سیستم‌های تشخیص نفوذ، به دو نوع سیستم‌های مبتنی بر شبکه و سیستم‌های مبتنی بر میزبان دسته‌بندی می‌شوند [10].

با فرض انتزاع لایه‌ای پروتکل SOAP از پروتکل‌های لایه کاربرد شبکه [6]، مشاهده می‌شود که سیستم‌های تشخیص نفوذ رایج، قادر به شناسایی حملات اختصاصی سرویس‌های وب نیستند. چراکه اصولاً توانایی درک محتوای اطلاعاتی در سطح سرویس را ندارند. بنابراین با وجود این نقص و آمار بالای حملات، تشخیص نفوذ در این سطح نیز ضروری است. این تحقیق در راستای تأمین امنیت سرویس‌های وب، با استفاده از روشهای خارج از سرویس صورت گرفته است. با توجه به خلأ موجود، یک معماری سیستم تشخیص نفوذ برای سرویس‌های وب ارائه می‌دهیم.

معماری پیشنهادی از چند جنبه قابل توجه است. اول اینکه برای پوشش سرویس‌های وب متعددی که در شبکه فعال هستند، از ساختار توزیع شده استفاده می‌شود. به‌علاوه این ساختار امکان کاستن بار پردازشی در واحد اصلی تشخیص نفوذ را که می‌تواند منجر به حمله انکار سرویس علیه خود سیستم تشخیص نفوذ شود، فراهم می‌نماید. از طرفی کنترل، نظارت و به‌روزرسانی‌های بانک‌های اطلاعاتی عامل‌های ناظر بر سرویس‌ها، به‌سهولت قابل انجام است. علاوه براین، با به‌کار گرفتن دو مکانیزم تشخیص نفوذ ناهنجاری و بدرفتاری، دقت تشخیص و نرخ خطای بهینه‌تری را دارا است.

ادامه مطالب این مقاله به این صورت سازماندهی شده‌اند: در بخش دوم به کارهای مرتبط در زمینه تشخیص نفوذ در لایه کاربرد و سطح سرویس اشاره می‌شود. برای درک بهتر حوزه فعالیت کارهای انجام شده در این بخش، باتوجه به منابع جمع‌آوری اطلاعات و داده‌های مورد پردازش سیستم‌های تشخیص نفوذ، در سه دسته از آنها نام برده می‌شود. در بخش سوم، به دانش پایه مورد نیاز اشاره می‌شود؛ مختصری در مورد سرویس‌های وب، سیستم‌های تشخیص نفوذ و حملاتی که روی سرویس‌های وب انجام می‌شود، بیان می‌شود. در بخش چهار، جایگاه و معماری سیستم تشخیص نفوذ پیشنهادی برای سرویس‌های وب، فازهای مختلف اجرا و نحوه تشخیص نفوذ، توضیح داده خواهد شد. بخش پنج نیز نتیجه‌گیری و کارهای آتی را شامل می‌شود.

۲- کارهای مرتبط

با مروری بر کارهای انجام شده در حوزه سیستم‌های تشخیص نفوذ حساس به محتوای وب، با توجه به مکان حمله، اطلاعات ممیزی، رخدادهای مورد بررسی و پروتکل‌های ارتباطی، این سیستم‌ها را در سه دستهٔ تشخیص نفوذ در خدمات‌دهنده وب، برنامه‌های کاربردی تحت وب و سرویس‌های وب، نام می‌بریم. هرچند اشتراک‌های زیادی بین این سه گروه وجود دارد، ولی تمیز جایگاه هریک می‌تواند به درک اهمیت تشخیص نفوذ در سرویس‌های وب کمک نماید.

سیستم‌های تشخیص نفوذ در خدمات‌دهنده‌های وب عموماً از محتوای سرآیند پرس و جوهای HTTP، متدهای مورد استفاده آن و فایل گزارش خدمات‌دهنده وب، قادر به تشخیص حملات وبی هستند. کارهایی نظیر WebSensorIDS [15]، WebSTAT [16] و Snort [14] در این دسته قرار می‌گیرد. تلاشهای زیادی برای

[1] Parsing
[2] Schema
[3] Misuse
[4] Anomaly
[5] Profile
[6] Specification-based

تشخیص نفوذ در برنامه‌های کاربردی تحت وب روی خدمات‌دهنده-های وب مثل [17، 18، 19] نیز انجام شده است که با توجه به محل و منابع جمع‌آوری اطلاعات در آنها، در این دسته قرار می‌گیرند.

دسته دوم سیستم‌های تشخیص نفوذ در این سطح، برنامه‌های کاربردی وبی را هدف جمع‌آوری اطلاعات نفوذ قرار می‌دهند [20، 21، 22]. روشهای ارائه شده در این دسته همگی بدنبال راهی برای تشخیص نفوذ در برنامه‌کاربردی تحت وب هستند. این دسته به‌دنبال حفاظت از خود برنامه کاربردی تحت وب مستقل از خدمات‌دهنده وب است. هرچند برای تشخیص بهینه، از اطلاعات موجود در خدمات‌دهنده وب نیز استفاده می‌کنند.

دسته سوم، سیستم‌های تشخیص نفوذ خاص سرویس‌های وب هستند. تا زمان این تحقیق در حوزه تشخیص نفوذ در سطح سرویس وب کارهای کمی انجام شده است. شاید بشود از پروژه mod security [13]، به‌عنوان نزدیکترین کار در این خصوص نام برد؛ که در اصل آن نیز یک دیوارآتش برنامه‌کاربردی تحت وب[1] (WAF) است که امکان تشخیص نفوذ نیز در آن افزوده شده است. سایر کارهای انجام شده مثل [23، 24]، در این حیطه بیشتر به جنبه تئوری و نظری قضیه پرداخته‌اند.

طراحی و پیاده‌سازی سیستم‌های تشخیص نفوذ در سطح سرویس وب این مزیّت را نسبت به انواع دیگر داراست که، به‌دلیل استفاده سرویس‌های وب از استانداردها، ساده‌تر و امکان‌پذیرتر است و طبیعتاً پیچیدگی‌های تشخیص نفوذ در برنامه‌های کاربردی، که فناوری و کاربرد آنها از فراوانی و تنوع بسیاری برخوردار است را ندارد. در ضمن توسعه برنامه‌های کاربردی تحت وب در آینده نزدیک به سوی استفاده از سرویس‌های وب است و با پیدایش Web2 و Web3 سیستم‌های تشخیص نفوذ در این سطح، مؤثر هستند. از طرفی، ناکارآمدی سیستم‌های تشخیص نفوذ در سطوح دیگر در تأمین نیاز سرویس‌های تحمل‌پذیر در برابر نفوذ، اهمیت سیستم‌های تشخیص نفوذ خاص سرویس‌های وب را پررنگ‌تر می‌کند [39].

۳- دانش اولیه

در این بخش پیشینه اطلاعاتی مورد نیاز برای ارائه معماری پیشنهادی بیان می‌شود. مفاهیمی چون سرویس‌های وب و فناوریهای آن، مروری بر سیستم‌های تشخیص نفوذ، مؤلفه‌های آن، انواع روشهای تشخیص و مزایا و معایب هریک و حملاتی که روی سرویس‌های وب انجام می‌شود به صورت اجمالی نام برده می‌شود.

۳-۱ سرویس‌های وب

تعاریف مختلفی در مراجع گوناگون از سرویس‌های وب وجود دارد. اما طبق [25] سرویس وب سیستمی نرم‌افزاری است برای حمایت از قابلیت همکاری فعل و انفعالهای[2] ماشین به ماشین در شبکه. سرویس وب دارای یک رابط، با توصیفی قابل پردازش برای ماشین (WSDL) است. سیستم‌های دیگر به‌وسیله پیامهای SOAP با سرویس وب با توصیف فوق، دارای فعل و انفعال هستند که نوعاً از HTTP به‌همراه دنباله‌ای از اسناد XML در پیوستگی با دیگر استانداردهای مرتبط با وب، انتقال می‌یابند. البته باید اضافه نمود که سرویس‌های وب از دیگر پروتکل‌های لایه کاربرد نیز برای انتقال می‌توانند استفاده نمایند.

به‌طورکلی سرویس‌های وب بر پایه فناوری XML [26] استوارند. سرویس‌های وب اطلاعات را در قالب اسناد XML انتقال می‌دهند. با امکاناتی که XML دارد، خود را توصیف و در دسترس عموم قرار می‌دهند. پروتکل SOAP، با ساختاری که بر اساس XML ایجاد می‌شود، وظیفه انتقال اطلاعات را به‌خوبی انجام می‌دهد [27]. برای استفاده از سرویس‌های وب نیاز به اطلاعاتی در مورد آنها است. پارامترهای ورودی و خروجی، پروتکل انتقال (مثل HTTP، MIME، FTP و غیره) برای ارتباط با سرویس وب و موارد دیگر، در توصیفی که از سرویس وب در هنگام ایجاد آن ساخته می‌شود، بیان می‌گردد. این مجموعه توصیفات در یک فایل دارای قالب XML به نام WSDL است [28]. برنامه‌های کاربردی تحت وب برای جستجوی سرویس مورد استفاده، به مکانی برای کاوش نیاز دارند؛ با استفاده از UDDI امکان جستجوی سرویس‌های وب فراهم می‌شود [29].

۳-۲ سیستم‌های تشخیص نفوذ

طبق [30، 31] نفوذ عبارت است از تلاشهایی برای به مصالحه انداختن محرمانگی، جامعیت، قابلیت دسترسی یا دور زدن مکانیزم‌های امنیتی یک کامپیوتر یا شبکه. تشخیص نفوذ، فرآیند نظارت بر رخدادها در یک شبکه یا سیستم کامپیوتری و تحلیل آنها برای یافتن نشانه‌هایی از نفوذ است. سیستم‌های تشخیص نفوذ نیز سیستم‌های نرم‌افزاری یا سخت‌افزاری هستند که فرآیند نظارت بر رخدادها در شبکه یا سیستم‌های کامپیوتری را به‌طور خودکار انجام می‌دهند.

از دیدگاه‌های مختلف دسته‌بندی‌های متفاوتی برای سیستم‌های تشخیص نفوذ می‌توان ارائه داد. دو منظر دسته‌بندی عبارتند از مدل پردازشی و منابع اطلاعاتی. مدل پردازشی با رویکرد نحوه تشخیص و انجام تحلیل‌های نفوذ، سیستم‌های تشخیص نفوذ را به سه دسته تشخیص ناهنجاری، بدرفتاری و مبتنی بر مشخصه تقسیم می‌کند. البته از روشهای ترکیبی نیز برای حصول دقت بالاتر در تشخیص و تولید خطای کمتر در طراحی سیستم‌های تشخیص نفوذ استفاده می‌شود.

تشخیص بدرفتاری یا تشخیص مبتنی بر امضاء از الگوی حملات شناخته شده - که به آنها امضاء گفته می‌شود – استفاده می‌کند. این روش منجر به تولید خطای تشخیص کمی می‌شود و به همین

[1] Web Application Firewall
[2] Interaction

دلیل در اکثر محصولات تجاری به‌کار گرفته می‌شود. اشکال بزرگی که وجود دارد، ناتوانی این روش در تشخیص حملات جدیدی است که هنوز الگویی برای آن ایجاد نشده است. بنابراین به‌روز نگه داشتن بانک اطلاعاتی الگوی حملات در این سیستم‌ها، اهمیت بسیار بالایی در کارایی آن دارد.

اما روش تشخیص ناهنجاری، به دنبال یافتن رفتارهای مشکوک و غیرعادی با مقایسه با رفتارهای نرمال است. رفتارهای نرمال با ایجاد نمایه‌ها[1]در سیستم ایجاد می‌شوند. معمولاً نمایه‌های ایجاد شده تنها درصدی از رفتارهای قانونی را پوشش می‌دهند و از اینرو تخطی از آنها، با یک تخمین به‌عنوان نفوذ در نظر گرفته می‌شود. لذا، این روش قابلیت آن را دارد که حملات جدید را تشخیص دهد، ولی خطای تشخیص نسبتاً زیادی تولید می‌نماید [31، 41].

رهیافت تشخیص نفوذ مبتنی بر مشخصه، به‌عنوان روشی برای ترکیب ویژگی‌های دو روش فوق مطرح شده است. در این روش معیارها یا مشخصه‌های سیستم یا شبکه، به عنوان رفتارهای عادی و قانونی، به‌طور دستی استخراج می‌شوند. از اینرو معیاری برای تشخیص نفوذ حاصل می‌شود. این روش هم ابهاماتی مثل پیچیدگی و زمان‌بری استخراج الگوهای رفتاری سیستم، متناسب با منبع مورد استفاده، یا عدم تشخیص حملاتی که بر مبنای رفتارهای عادی سیستم هستند را داراست [32، 33].

از دیدگاه منابع اطلاعاتی نیز سیستم‌های تشخیص نفوذ را به دو دسته عمده سیستم‌های مبتنی بر میزبان و مبتنی بر شبکه می‌توان تقسیم نمود. اطلاعات و پردازش‌ها در صورتی که در میزبان باشند جزء دسته اول اشت که در این صورت IDS به صورت یک بسته نرم‌افزاری در ماشین میزبان نصب می‌شود. در حالی که دسته دوم، اطلاعات را از ترافیک شبکه و عامل‌ها و حسگرهایی که در بخشهای مختلف شبکه توزیع شده‌اند جمع‌آوری می‌کند. در این منظر نیز حالت‌های ترکیبی وجود دارد. در این صورت سیستم تشخیص نفوذ می‌تواند دید جامعی از منابع تحت نظارت خود داشته باشد [10، 31].

۳-۳ حملات سرویس‌های وب

هدف نفوذگر از حمله به سرویس وب، به مصالحه انداختن آن برای دسترسی غیرمجاز به منابعی چون سیستم فایل، بانک‌های اطلاعاتی و دیگر سرویس‌های پشت آنها است و در بدترین حالت، نفوذگر سعی در جهت از کار انداختن سرویس می‌نماید.

حملاتی چون سرریز بافر، انکار سرویس، تزریق کد، XSS در سرویس‌های وب رایج هستند. هر یک از موارد برشمرده نیز خود به روشهای مختلفی اجرا می‌شوند. کارهای مختلفی روی طبقه‌بندی حملات سرویس‌های وب انجام شده است که از آن جمله می‌توان به [34، 35، 36، 37] اشاره کرد. اما نکته مهم در مورد تشخیص حملات سرویس‌های وب، مکان اثر حمله و نحوه اجرای آن است. یعنی حمله با چه هدفی اجرا می‌شود و بر اساس چه عمل‌هایی شکل می‌گیرد. اینکه چه مواردی را باید تحت مراقبت قرار دهیم، یا با بررسی چه رخدادهایی یا دنباله‌ای از وقایع، پی به وقوع حمله خواهیم برد، ما را در تشخیص نفوذ یاری می‌رساند.

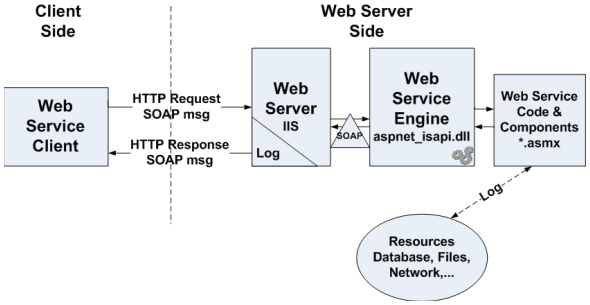
۴- معماری پیشنهادی

هرچند امروزه تشخیص دقیق یک حمله نیازمند همکاری سیستم‌های تشخیص نفوذ در لایه‌های مختلف شبکه، میزبان و حتی سرویس‌ها است؛ هدف از این تحقیق تشخیص نفوذ در سرویس‌های وب است و فرض بر آن است که، نفوذگر به منظور مصالحه کردن یا از کار انداختن سرویس وب، حمله خود را طرح‌ریزی می‌کند. تشخیص نفوذ در لایه‌های دیگر شبکه یا میزبان به‌عهده سیستم‌های موجود است و به‌عنوان سطح دیگری از امنیت، سیستم تشخیص نفوذ برای سرویس‌های وب پیشنهاد می‌شود. از اینرو، شناخت سرویس وب و تمرکز در پیامهای SOAP، به‌عنوان راه دسترسی خارجی به سرویس‌ها، فرضهای اصلی هستند که در این پژوهش مد نظر قرار گرفتند. در این بخش پس از بیان جایگاه سیستم و منابع اطلاعاتی مورد نیاز، بلوک‌های سازنده سیستم تشخیص نفوذ ترسیم و معرفی می‌شود. سپس فازهای عملیاتی سیستم و نحوه کارکرد اجزای آن تشریح می‌گردد.

۱-۴ جایگاه سیستم

در این بخش از دو جهت جایگاه سیستم تشخیص نفوذ در سرویس‌های وب که برای سادگی از این پس WS-IDS نامیده می‌شود را بررسی می‌کنیم: اول، مکان سرویس‌های وب به عنوان موضوع امنیت و دوم، جایگاه توپولوژیکی سیستم.

با مراجعه به شکل (۱) - به عنوان مثال در فناوری NET. با الگو برداری از [7] - محل سرویس وب در خدمات دهنده وب را مشخص می‌نماییم.

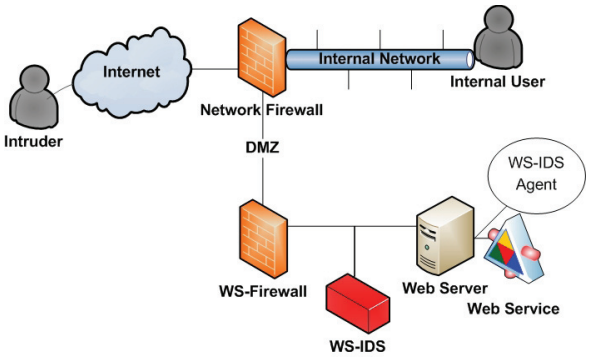


شکل ۱: جایگاه سرویس وب در خدمات دهنده وب

خدمات‌گیرنده سرویس وب با پروتکل HTTP که حاوی پیامهای SOAP است، به خدمات‌دهنده وب متصل، و تقاضاهای خود را

[1] Profiles

ارسال و دریافت می‌دارد. خدمات‌دهنده وب (IIS)، محتوای SOAP را دریافت و به مؤلفه سیستمی سرویس وب (aspnet_iaspi.dll) انتقال می‌دهد. سرویس وب از طریق این مؤلفه، درخواست‌های وارده را پاسخ می‌دهد. متناسب با کارکرد سرویس وب، امکان دسترسی به منابعی چون بانک‌های اطلاعاتی، فایل‌ها و فهرست‌ها یا سایر منابع شبکه وجود می‌تواند داشته باشد. شکل (۲) جایگاه WS-IDS را در شبکه نشان می‌دهد.



شکل ۲: محل قرار گیری سیستم تشخیص نفوذ سرویس وب بعد از دیوار آتش XML به صورت غیرفعال

مطابق شکل (۲)، WS-IDS دو جزء عملیاتی مجزا روی ماشین خدمات دهنده وب و واحد مرکزی متصل به شبکه دارد. همچنین قبل از سرویس وب، دیوارآتش XML وجود دارد که ترافیک نامطمئن ورودی از اینترنت را به ترافیک مطمئن تبدیل می‌نماید [9، 38]. برای تشخیص نفوذ در چنین سطحی، لازم است که بر منابع برخط و نابرخطی، مانند فایل‌های گزارش خدمات دهنده وب و سرویس وب و پیامهای درخواست و پاسخ SOAP نظارت داشت.

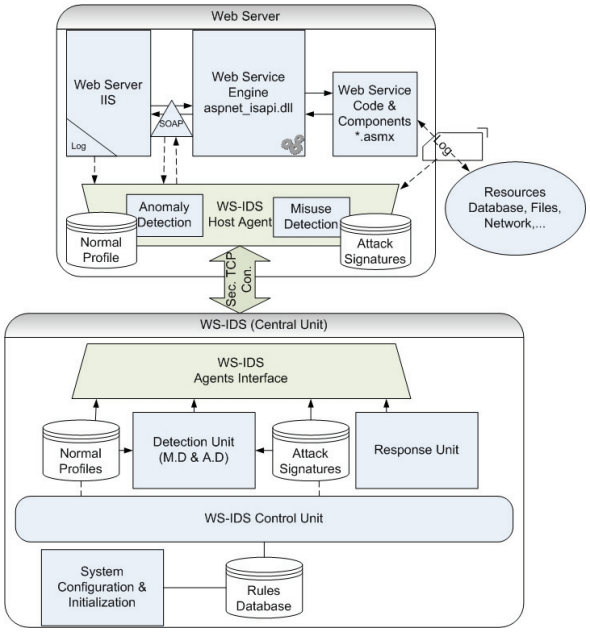
در صورتی که نفوذگر بتواند به طریقی مکانیزم‌های امنیتی دیوار آتش XML را دور بزند، WS-IDS قادر است با نظارت بر پیامهای SOAP حمله در حال وقوع را تشخیص داده؛ هشدارهای لازم را برای پیگیری آتی مدیر شبکه تولید نماید.

۲-۴ معماری پیشنهادی

مطابق با رهنمودهای موجود در اجزای سازنده سیستم‌های تشخیص نفوذ مثل [30، 31، 43]، این معماری دارای مؤلفه‌هایی از قبیل عامل‌ها، واحد تحلیل، واحد پاسخ و بانک‌های اطلاعاتی مورد نیاز سیستم است.

از آنجایی که همواره سرویس‌های وب در معرض حملات جدید هستند، بنابر این لازم است که WS-IDS توانایی تشخیص رفتارهای مشکوک را دارا باشد. از طرفی با در نظر گرفتن امضاء حملات شناخته شده، از تولید زیاد پیامهای خطای تشخیص کاسته بشود. از اینرو، رهیافت دوگانه تشخیص ناهنجاری و تشخیص بدرفتاری، برای بهره‌گیری از مزایای هر دو روش در معماری پیشنهادی استفاده می‌شود. شکل (۳) بخشهای WS-IDS را در خدمات‌دهنده وب و واحد مرکزی نشان می‌دهد.

معماری WS-IDS به‌صورت توزیع‌شده، در خدمات‌دهنده وب و واحد مرکزی است. مزیّت این مدل با توجه به حجم پیامهای مبادله شده به سمت سرویس وب، کاستن از ترافیک در بخش مرکزی و پیشگیری از حمله انکار سرویس به آن است.



شکل ۳: بخشهای WS-IDS در خدمات دهنده وب و واحد مرکزی

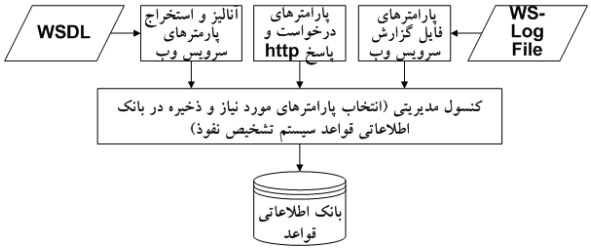
عامل نرم‌افزاری نصب‌شده در خدمات‌دهنده، در اصل یک سیستم تشخیص نفوذ با سربار کم است که به‌طور محلی عملیات تشخیص را انجام می‌دهد. هر دو بخش دارای دو بانک اطلاعاتی هستند که الگوی حملات و نمایه‌های عادی را برای تشخیص بدرفتاری و ناهنجاری نگهداری می‌کنند. اصول تشخیص در دو بخش سیستم یکسان است. ارتباط بین بخشهای سیستم نیز با استفاده از اتصال امن TCP - مثل SSL - برقرار می‌شود.

واحد مرکزی متشکل است از بلوک‌های کنترلی، تشخیص، پاسخ، واسط عامل‌ها و بانک‌های اطلاعاتی نمایه‌های نرمال، الگوی حملات و قواعد سیستم، و واحد تنظیم و شروع مجدد. در ادامه نحوه کارکرد سیستم بیان می‌شود.

۳-۴ زمان اجرای سیستم

زمان اجرای سیستم مرکب است از سه فاز تنظیم و مقداردهی اولیه، آموزش و تشخیص. در هنگام تنظیم و مقداردهی اولیه، WS-IDS با دریافت فایل WSDL پارامترهای سرویس وب را شناسایی و به همراه دیگر پارامترهای مورد نیاز در خدمات‌دهنده وب، آیتم‌های لازم جهت نظارت توسط عامل‌ها را در بانک اطلاعاتی قواعد خود ذخیره می‌نماید. شکل (۴) نحوه تنظیم و

مقداردهی اولیه را نشان می‌دهد. در این مرحله سیستم با نظارت مستقیم مدیر شبکه عمل می‌نماید.



شکل ۴: تنظیم و مقداردهی اولیه سیستم WS-IDS

با دریافت فایل WSDL پارامترهای سرویس وب استخراج و مدیر سیستم می‌تواند موارد خاصی را برای پیگیری و نظارت سیستم انتخاب نماید. همچنین درصورتی که فایل گزارشی از فعالیت‌های سرویس وب ثبت می‌شود، فیلدهای مناسب آن برای ممیزی انتخاب می‌شوند. برای تشخیص مؤثرتر حملات، آیتم‌های مناسبی که در خدمات‌دهنده وب ثبت می‌شوند نیز برگزیده می‌شوند. در نهایت در بانک اطلاعاتی قواعد WS-IDS ساختار داده‌ای از رکوردهای مختلف مطابق توصیفات جدول (۱) ایجاد می‌شود.

فاز آموزش، پس از مقداردهی و تنظیمات اولیه اجرا می‌گردد که در طی آن سیستم، رفتارهای عادی سرویس وب را با استفاده از داده‌های آموزشی ارزیابی و دسته‌بندی می‌کند. عامل موجود در خدمات‌دهنده وب صرفاً به صورت یک حسگر عمل می‌نماید و درخواست/پاسخ‌ها را در قالب ساختار داده تعیین شده در فاز قبل، مستقیماً برای واحد مرکزی ارسال می‌کند.

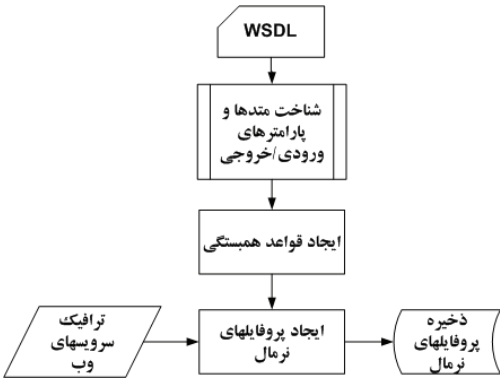
جدول ۱ : فیلدهای ساختار داده عامل سیار

نام فیلد	توضیح	محل استخراج
web_srv_ID	شناسه خدمات دهنده وب	مقداردهی اولیه در WS-IDS
host_IP	شناسه میزبان (مشتری) متصل به خدمات دهنده وب	فایل گزارش خدمات دهنده وب
http_req_param	پارامترهای مورد توجه برای بازرسی در درخواست وب	فایل گزارش خدمات‌دهنده وب
soap_req_msg	پارمترهای مورد توجه برای بازرسی در پیام درخواست SOAP	مقداردهی اولیه در WS-IDS و فایل WSDL
ws_log_content	پارامترهای مورد توجه در بازرسی فایل گزارش سرویس وب	مقداردهی اولیه در WS-IDS و فایل گزارش سرویس وب در خدمات‌دهنده وب
http_res_param	پارامترهای مورد توجه برای بازرسی در پاسخ به درخواست وب	فایل گزارش خدمات‌دهنده وب
soap_res_msg	پارامترهای مورد توجه برای بازرسی در پاسخ به درخواست SOAP	مقداردهی اولیه در WS-IDS و فایل WSDL
ws_tag	تگ سرویس وب در حالتی که بیش از یک سرویس وب در یک خدمات‌دهنده موجود باشد	مقداردهی اولیه در WS-IDS

هدف از ایجاد نمایه‌های نرمال سیستم، ایجاد مبنایی برای تشخیص رفتارهای مشکوک و غیرعادی است که از سرویس وب یا درخواست‌دهنده سر می‌زند. از اینرو، روشهای تشخیص ناهنجاری و داده کاوی یا استخراج دانش [40، 43] برای دسته‌بندی رفتارهای درخواست‌دهنده و سرویس وب مناسب هستند. به‌عنوان نمونه با سودجستن از قواعد همبستگی ارتباط و توالی بین پارامترهای ورودی و خروجی سرویس وب مشخص می‌شود. شکل (۵) این مطلب را نشان می‌دهد.

پس از تکمیل فاز آموزش، بانک اطلاعاتی الگوهای حمله برای تشخیص بدرفتاری به همراه آخرین تغییرات به‌روز می‌شود. سپس نمایه‌ها و الگوی حملات برای به‌هنگام‌سازی پایگاه‌داده‌های عامل مستقر در خدمات دهنده ارسال می‌شود.

اکنون سیستم WS-IDS آماده تغییر وضعیت به فاز تشخیص است. در این فاز، ابتدا تشخیص بدرفتاری با بررسی انطباق ترافیک عبوری به سرویس‌های وب با الگوی حملات به صورت فعال در خدمات دهنده، توسط عامل WS-IDS انجام می‌شود. در صورتی که حمله‌ای تشخیص داده شد، اطلاعات پیام درخواست مشکوک به سیستم مرکزی برای تولید هشدار و ثبت در بانک اطلاعات مجزایی، ارسال می‌شود. همچنین در صورت لزوم، عامل قادر به مسدود کردن ترافیک بدخواه است.



شکل ۵: توصیف اجمالی از فاز آموزش با استفاده از قواعد همبستگی برای ایجاد نمایه‌های نرمال

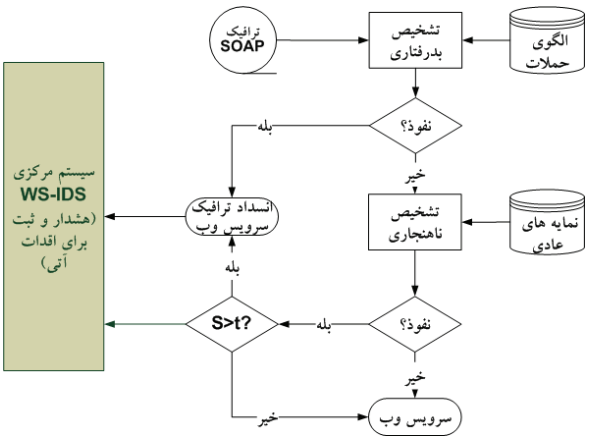
تشخیص ناهنجاری بعد از تشخیص بدرفتاری صورت می‌گیرد. به‌دلیل عدم قطعیت در تشخیص ناهنجاری، سیاست محافظه‌کارانه‌ای نسبت به تشخیص بدرفتاری در نظر گرفته می‌شود. در صورت مشاهده ترافیک مشکوک از سوی عامل، متناسب با قواعد تنظیم شده، پیامهای درخواست و پاسخ به‌همراه سایر اطلاعات اضافه، به سیستم مرکزی ارسال می‌شود.

معمولاً در تشخیص ناهنجاری، بسته به نوع الگوریتم تشخیص، حد آستانه‌ای برای نفوذ در نظر گرفته می‌شود. در صورتی که رفتاری مشکوک مشاهده شود، با محاسبه امتیاز ناهنجاری آن با آستانه نفوذ مقایسه می‌شود. اگر آستانه نفوذ از امتیاز ناهنجاری کمتر

باشد، از رسیدن پیامهای درخواست به سرویس وب جلوگیری می‌شود، در غیر این صورت ترافیک مجاز به اخذ سرویس است.

در واحد مرکزی سیستم، علاوه بر ثبت اطلاعات رفتارهای مشکوک، مدیر سیستم بر آنها نظارت می‌نماید تا سیاست‌های لازم برای تشخیص مثل آستانه نفوذ و نرخ تشخیص بازبینی شود. شکل (۶) روند مراحل فوق را نشان می‌دهد. در این شکل S امتیاز ناهنجاری است که در ترافیک سرویس وب محاسبه می‌شود و t آستانه نفوذ است.

در واحد مرکزی سیستم WS-IDS می‌توان یک بانک اطلاعاتی دیگری برای ثبت ترافیک‌های مشکوک ایجاد کرد یا اطلاعات ترافیکی مشکوک را به سیستم پاسخ به نفوذ در شبکه ارسال نمود[41]. در این صورت امکان تحلیل داده‌های جمع شده برای تشخیص الگوی حملات جدیدتر یا ارتباط با دیگر سیستم‌های تحلیل داده در شبکه برای تشخیص و پیشگیری از حملات خاص و گسترده بوجود می‌آید.



شکل ۶: زمان اجرای فاز تشخیص عامل خدمات دهنده

معماری پیشنهادی با توجه با ساختار توزیع شده در خدمات‌دهنده‌هایی که سرویس‌های وب در آنها نصب هستند، قابلیت تشخیص نفوذ به صورت محلی را داراست و می‌تواند از بروز آسیب‌های جدی به سیستم بلافاصله بعد از تشخیص جلوگیری کند. همچنین این سیستم امکان استفاده از سایر تجهیزات حساس به XML به‌عنوان عامل حسگر را دارد؛ از اینرو با چنین ترکیبی از حسگرهای مختلف در بخشهای متفاوت شبکه، قادر به تشخیص دقیق‌تر حملات در سطح سرویس است.

۵- نتیجه‌گیری و کارهای آینده

در این مقاله ابتدا یک دسته‌بندی از کارهای انجام شده در حوزه سیستم‌های تشخیص نفوذی که در لایه کاربرد مدل مرجع شبکه فعالیت می‌کنند ارائه شد. سرویس‌های وب به‌دلیل اهمیت و توسعه در کاربرد آنها نیازمند سیستم‌های حفاظتی خاص خود هستند. از اینرو سیستم تشخیص نفوذی که قادر به فعالیت در این سطح باشد ضروری است. در این مقاله یک معماری برای این گونه سیستم‌ها ارائه شد. رهیافت‌های تشخیص از سیستم‌های تشخیص مبتنی بر شبکه و میزبان وام گرفته و شامل تشخیص ناهنجاری و تشخیص بدرفتاری طبق یک ساختار توزیع شده است. با استفاده از این معماری مکان فناوری‌های لازم برای جمع‌آوری اطلاعات، تشخیص بهینه و پاسخ مشخص شده‌اند. این معماری می‌تواند مبنایی برای تحقیق و توجه بیشتر در حوزه پیدایش سیستم‌های تشخیص نفوذ در سطح سرویس وب باشد.

در راستای توسعه و بهبود معماری ارائه شده در این پژوهش و با توجه به دیدگاه جدیدی که ارائه شد، کارهای بسیاری قابل انجام است. از آن دست می‌توان به مواردی چون، بهبود در مکانیزم جمع‌آوری اطلاعات با توسعه حسگرها به ابزارهای حساس به XML مثل دیوارآتش XML، مسیریاب و توزیع بار سرویس وب، XML Proxy، کاوش برای یافتن الگوریتم‌های بهینه تشخیص نفوذ در مستندات XML با رهیافت‌های تشخیص ناهنجاری و بدرفتاری، ایجاد روشهایی برای تولید خودکار الگوی حملات پس از کشف نفوذ، بررسی مسائل کارایی و انجام‌پذیری با روشهای صوری، مدلسازی و شبیه‌سازی و پیاده‌سازی نمونه اولیه از محصول و بررسی نتایج عملی، اشاره کرد. همچنین کار در حوزه سیستم‌های پیشگیری از نفوذ و پاسخ به نفوذ نیز می‌تواند افقهای جدیدی روی این کار بگشاید.

مراجع

[1] M. Stal, "Web Services: Beyond Component-based Computing," in *Communications of the ACM*. vol. 45: ACM, 2002, pp. 71-78.

[2] W3C, URL: http://www.w3c.org/

[3] OASIS, URL: http://www.oasis-open.org/

[4] K. Tang, S. Chen, J. Zic, and B. Yan, "A Performance Evaluation of Web Services Security," in *Enterprise Distributed Object Computing Conference (EDOC'06)*. vol. 10th IEEE, Hong Kong, 2006, pp. 67-74.

[5] Basic Security Profile Version 1.0, URL: http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2007-03-30.html

[6] R. Bunge, et al., "An Operational Framework for Service Oriented Architecture Network Security," in *Proc. of the 41st Annual Hawaii Int'l Conf. on System Sciences,* IEEE, 2008, pp. 312-312.

[7] S. Shah, *Hacking Web Services*, 1st ed. Boston, Massachusetts: Charles River Media, 2007.

[8] Y. S. Loh, et al., "Design and Implementation of an XML Firewall," in *Proc. of the 2006 Int'l Conf. on Computational Intelligence and Security,* IEEE, Guangzhou, 2006, pp. 1147-1150.

[9] M. Holtkamp, "The Role of XML Firewalls for Web Services," *The 1st Twente Student Conference on IT*, Track B, June 2004.

[10] J. Pieprzyk, T. Hardjono, and J. Seberry, "Intrusion Detection," in *Fundamentals of Computer Security*, Springer, 2003, pp. 321-347.

[11] Z. Li, A. Das, and J. Zhou, "Theoretical Basis for Intrusion Detection," *Proc. of 6th IEEE Information Assurance Workshop (IAW)*, June 15-17, West Point, NY., 2005.

[12] Web Application Security Consortium, URL: http://www.webappsec.org/projects/whid/

[13] mod security, URL: http://www.modsecurity.org/

[14] Snort, URL: http://www.snort.org/

[15] J. Dong, "SensorWebIDS: A Sensor with Misuse and Anomaly Based Data Mining Technique for Web Intrusion Detection," Master Thesis, Ontario, Canada: Windsor, 2006, p. 95.

[16] G. Vigna, W. Robertson, V. Kher, and R. A.Kemmerer, "A Stateful Intrusion Detection System for World-Wide Web Servers," in *Proc. of the 19th Annual Computer Security Applications Conference (ACSAC'03)*: IEEE, 2003, pp. 1-10.

[17] C. Kruegel, G. Vigna, and W. Robertson, "A Multi-Model Approach to the Detection of Web-Based Attacks," in *Computer Networks*. vol. 48: Elsevier, 2005, pp. 717-738.

[18] K. L. Inghman, A. Somayaji, J. Burge, and S. Forrest, "Learning DFA representations of HTTP for protecting web applications," in *Computer Networks*. vol. 51: Elsevier, 2007, pp. 1239-1255.

[19] Y. Park and J. Park, "Web Application Intrusion Detection System for Input Validation Attack," in *Proc. of the 3rd 2008 Int'l Conf. and Hybrid Information Technology*, 2008, pp. 498-505.

[20] C. G. Yee and G. S. V. R. K. Rao, "A Hybrid Approach to Intrusion Detection and Prevention for Business Intelligence Applications," in *ISCIT*: IEEE, 2006, pp. 847-850.

[21] J. J. G. Adeva and J. M. P. Atxa, "Intrusion Detection in Web Applications Using Text Mining," in *Engineering Applications of Artificial Intelligence*, vol. 20: Elsevier, 2006, pp. 555-566.

[22] M. Cova, et al., "Swaddler: An Approach for the Anomaly-based Detection of State Violations in Web Applications," in *Proc. of the 10th Int'l Symp. on Recent Advances in Intrusion Detection (RAID'07)*, 2007, pp. 63-86.

[23] C. G. Yee, W. H. Shin, and G. S. V. R. K. Rao, "An Adaptive Intrusion Detection and Prevention (ID/IP) Framework for Web Services," in *Proc. of the Int'l Conf. on Convergence Information Technology (ICCIT)*: IEEE Computer Society, 2007, pp. 528-534.

[24] J. Wang and L. L. IACONO, "Intrusion Detection and tolerance in Grid-based applications," in *Proc. of the 3rd In'l Conf. in Security and Privacy in Communications Network and the Workshop (SecureComm'07)*: IEEE, 2007, pp. 177-185.

[25] Web Services Glossary, W3C Working Group Note 11 February 2004, URL: http://www.w3.org/TR/ws-gloss/

[26] Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation 26, Nov. 2008, URL: http://www.w3.org/TR/2008/REC-xml-20081126/

[27] SOAP Version 1.2 Part 0: Primer (Second Edition), W3C Recommendation 27, April 2007, URL: http://www.w3.org/TR/2007/REC-soap12-part0-20070427/

[28] Web Services Description Language (WSDL) 1.1, W3C Note 15, March 2001, URL: http://www.w3.org/TR/2001/NOTE-wsdl-20010315

[29] "UDDI Version 3.0.2," in *UDDI Spec Technical Committee Draft*, L. Clement, A. Hately, C. v. Riegen, and T. Rogers, Eds.: OASIS, 2004, URL: http://uddi.org/pubs/uddi-v3.0.2-20041019.htm.

[30] R. Bace and P. Mell, "Intrusion Detection Systems (IDPS)", 2001, URL: http://purl.access.gpo.gov/GPO/LPS72073.

[31] K. Scarfone and P. Mell, "Guide to Intrusion Detection and Prevention Systems (IDPS), SP-800-94," National Institute of Standards and Technology (NIST), 2007.

[32] P. Uppuluri and R. Sekar, "Experiences with Specification-Based Intrusion Detection," in *Proc. of RAID 2001*, Springer, pp. 172-189, 2001.

[33] R. Sekar, et al., "Specification-based Anomaly Detection: A New Approach for Detecting Network Intrusions," in *Proc. of CCS'02* Washington, DC, USA: ACM, 2002, pp. 265-275.

[34] J. Seo, H.-S. Kim, S. Cho, and S. Cha, "Web Server Attack Categorization based on Root Causes and Their Locations," in *Proc. of the Int'l Conf. on Information Technology: Coding and Computing (ITCC'04):* IEEE Computer Society, 2004.

[35] A. Vorobiev and J. Han, "Security Attack Ontology for Web Services," in *Proc. of the 2nd Int'l Conference on Semantics, Knowledge, and Grid (SKG'06)*: IEEE Computer Society, 2006.

[36] E. Moradian and A. Hakansson, "Possible attacks on XML Web Services," *Int'l J. of Computer Science and Network Security (IJCSNS),* vol. 6, pp. 154-170, 2006.

[37] A. Singhal and T. Winograd, "Guide to Secure Web Services (Draft), SP 800-95," NIST 2006.

[38] D. Patterson, "XML Firewall Architecture and Best Practices for Configuration and Auditing," SANS Institute, 2007.

[39] Z. Aghajani and M. Abdollahi Azgomi, "A Multi-Layer Architecture for Intrusion Tolerant Web Services," *Int'l Journal of u- and e- Service, Science and Technology*, 2008, pp. 73-80.

[40] J. Han and M. Kamber, *Data Mining Concepts and Techniques*, Morgan Kaufmann Publishers, 2006.

[41] P. Kabiri and A. A.Ghorbani, "Research on Intrusion Detection and Response: A Survey," *International Journal of Network Security,* vol. 1, pp. 84-102, 2005.

[42] P. Garcia-Teodoro, et al., "Anomaly-based network intrusion detection: Techniques, systems and challenges," *Computer & Security,* vol. 28, Elsevier, 2009, pp. 18-28.

[43] Common Intrusion Detection Framework, 1998, URL: http://gost.isi.edu/cidf/drafts/communication.txt.