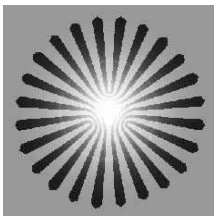


دانشگاه پیام نور

مرکز تهران

پایان‌نامه برای دریافت درجه کارشناسی ارشد

در رشته مهندسی کامپیوتر- نرم افزار

دانشکده فنی و مهندسی

گروه علمی فناوری اطلاعات و ارتباطات

عنوان پایان‌نامه:

به کارگیری شبکه اجتماعی در سیستم های تشخیص نفوذ

استاد راهنما:

دکتر عباس قائمی بافقی

استاد مشاور:

دکتر احمد فراهی

نگارش:

مهدی علیزاده ثانی

بهمن ۱۳۸۸

تصویب نامه

پایان نامه تحت عنوان:

که توسط مهدی علیزاده ثانی تهیه و به هیات داوران ارائه گردیده است مورد تایید می باشد.

تاریخ دفاع : ۱۳۸۸/۱۱/۲۹ نمره: ۱۸ درجه ارزشیابی: خوب

اعضای هیات داوران:

	نام و نام خانوادگی	هیات داوران	مرتبه علمی	امضاء
۱-	دکتر عباس قائمی بافقی	استاد راهنما		
۲-	دکتر احمد فراهی	استاد راهنمای همکار یا مشاور		
۳-	دکترحسین شیرازی	استاد ممتحن		
۴-	دکتر رضا عسکری مقدم	استاد ممتحن		
۵-	سهیلا حافظی	نماینده گروه آموزشی		

راهنمایی های ارزنده و عالمانهٔ اساتید ارجمند جناب آقای دکتر عباس قائمی در مقام استاد راهنما و جناب آقای دکتر فراهی در مقام استاد مشاور، شرط لازم برای کامیابی اینجانب در این راه بود. وظیفهٔ خود می دانم از بذل لطف و دقت نظر ایشان، قدردانی و تشکر صمیمانهٔ خود را ابراز نمایم.

بر خود واجب می دانم از همهٔ استادان عزیزی که در طول این دوره از محضرشان استفاده نموده‌ام، سپاسگزاری نمایم که در حقیقت امید به بهره گیری از ارشادات ایشان، به من جرأت ورود به این عرصه را داد. از خداوند منان خواهانم سایهٔ این بزرگواران را سالهای متمادی بر سر جامعهٔ علمی ما مستدام بدارد.

بی مناسبت نیست از همسر مهربان و فداکارم که با تشویق اینجانب و تحمل دشواریها، یاریگر و پشتیبان اینجانب در این راه بوده اند، سپاسگزاری و از خداوند بزرگ سلامت ایشان را طلب نمایم.

چکیده

در این پایان نامه با ترکیب سیستم های تشخیص نفوذ با شبکه اجتماعی معماری جدیدی ارایه گردیده، که در آن برای سیستم های تشخیص نفوذ در بستر شبکه اجتماعی امکان اشتراک دانش فراهم شده است.

این سیستم از یک دیدگاه در رسته سیستم های توزیع شده قرار می‌گیرد. اما به لحاظ عملکردی کاملا با آنها متفاوت می باشد. عمده‌ترین تفاوت آن در نحوه کسب دانش های جدید است. سیستم پیشنهادی که SNIDS نامگذاری گردیده است، بر مشکلاتی نظیر عدم توسعه پذیری، وجود نقطه شکست و محدودیت در نوع سیستم تشخیص نفوذ فایق می آید.

ابتدا با ارایه یک معماری توزیع شده مبتنی بر ساختار شبکه اجتماعی و قراردادن سیستم های تشخیص نفوذ به عنوان گره های این شبکه و همچنین تعریف پروتکل و ساختار ارتباطی، امکان اشتراک دانش فراهم آمده است. سپس سیستم پیشنهادی (SNIDS) شبیه سازی شده و با استفاده از دو سیستم تشخیص نفوذ کد باز به نام های Snort و Bro توسعه داده شده است. نتایج ارزیابی با استفاده از داده های DARPA2000 بر روی این سیستم نشان دهنده تاثیر اشتراک دانش در بهبود عملکرد سیستم های تشخیص نفود می باشد.

کلمات کلیدی

سیستم تشخیص نفوذ، شبکه اجتماعی، اشتراک دانش، خرد جمعی، سیستم‌های توزیع شده، امنیت شبکه

فهرست مطالب و پیوست ها

فهرست جداول

فهرست اشکال

فصل اول

مقدمه

با گذشت زمان هکرها هر چه بیشتر در تکنیک‌های خود خبره می شوند. آن‌ها اغلب روش‌های مختلف را با هم ترکیب می کنند به گونه‌ای که تشخیص را مشکلتر می نماید. از دیدگاه امنیت شبکه، نظارت ساده بر استفاده از پردازنده، I/O یا فعالیت‌های صورت گرفته بر روی فایلها کفایت نمی کند و مساله اصلی در این نوع نظارت حمله‌ها هستند که حتی اگر تشخیص داده شوند تا زمانی که فردی مداخله نکند ادامه می یابند.[Idt07].

یک نفوذ[1] را می‌توان تخریب امنیت برای بدست آوردن دسترسی به یک سیستم تعریف نمود. برای انجام این عمل ممکن است از چندین روش حمله استفاده و زمان بسیاری نیز سپری گردد. این گونه دسترسی‌های بدون مجوز به سیستم کامپیوتر یا شبکه اغلب برای تحقیق در مورد ضعف های سیستم برای حمله های آتی استفاده می شوند. دیگر اشکال نفوذ با هدف محدود کردن و یا حتی جلوگیری از دسترسی به یک سیستم کامپیوتری و یا شبکه صورت می گیرند.

به صورت عام همانطور که از نام یک سیستم تشخیص نفوذ پیداست، این سیستم‌ها توانایی شناسایی نفوذهای ممکن را دارند. از دیدگاه تخصصی‌تر، هدف از ابزارهای سیستم تشخیص نفوذ تشخیص حملات و استفاده های نادرست از سیستم‌های کامپیوتری و شبکه و اعلان هشدار جهت انجام اقدام مناسب در مقابل نفوذ تشخیص داده شده می باشند.[Idt07]

از زمان طرح سیستم های تشخیص نفوذ به عنوان یک عامل حفاظتی برای سیستم‌های کامپیوتری تاکنون طرح های مختلفی بر روی معماری و یا تکنیک های تحلیل داده‌ی این سیستم ها پیشنهاد شده است. به جز

[1] Intrusion

برخی نوآوری‌ها که باعث ایجاد دسته‌ی جدیدی از سیستم‌های تشخیص نفوذ گردیده است، سایر طرح ها بیشتر با هدف بهبود کارایی این سیستم ها مطرح شده است. این بهبودها معمولا در دو رسته دنبال شده است. بهبود کارایی در سرعت تشخیص نفوذ که بیشتر بر روی تکنیک‌های مختلف تمرکز شده است و رسته دیگر بهبود کارایی سیستم تشخیص نفوذ در دامنه تشخیص و گسترش پایگاه دانش می باشد که موضوع این تحقیق در رسته دوم قرار می گیرد.

شالوده ای که در این پایان نامه به عنوان بستر برای سیستم های تشخیص نفوذ مورد استفاده قرار گرفته است، شبکه اجتماعی می باشد. یک شبکه اجتماعی یک ساختار اجتماعی ایجاد شده توسط نودهایی است (هر کدام مستقل هستند) که بوسیله نوع خاصی از وابستگی متقابل مانند مقدار، دیدگاه، عقیده، تعاملات مالی، دوستی، خویشاوندی، تجارت و ... به هم پیوسته شده اند. ساختار نتیجه معمولا خیلی پیچیده می باشد.

تحلیلگران شبکه‌های اجتماعی به کل روابط شبکه، در قالب نودها و وابستگی ها می نگرند. نودها عامل‌های مستقلی درون شبکه هستند و وابستگی ها نمایش دهنده روابط بین این عامل ها می باشد.

امروزه از شبکه‌های اجتماعی در کاربردهای مختلفی استفاده می شود. به نمونه هایی از این کاربردها در ادامه اشاره شده است:

أ. نرم‌افزارهای کاربردی تجاری: NetMiner[Arr03]، InFLow[Emp05]

ب. جمع آوری داده‌های نظرسنجی‌ها از شبکه‌های اجتماعی: Onasurveys.com[Mar07]

ج. جمع‌آوری داده از گروه های خبری[1]: UNISoN[Bar02]

د. سیستم عامل Mac: SocNetV[Jud02]

ه. اتخاذ تصمیمهای گروهی[Asn03]

و. داده کاوی چت [Vil05]

ز. افزایش کارایی در انجمن های وبی[2] [Ann06]

[1] News Group

[2] Web Community

۱-۱ ضرورت انجام تحقیق

علی رغم فعالیتهای بسیاری که به منظور بهبود کارایی سیستمهای تشخیص نفوذ صورت گرفته است، اما همچنان این مساله به عنوان یکی از اساسی ترین معضلات در استفاده از سیستمهای تشخیص نفوذ به شمار می آید. زیرا که بکارگیری یک سیستم تشخیص نفوذ در یک شبکه، به دلیل پردازشهایی که بر روی بسته های شبکه صورت می گیرد، باعث کاهش کارایی سیستم می شود. لذا مساله افزایش کارایی سیستمهای تشخیص نفوذ مسالهای بسیار حایز اهمیت می باشد. از طرفی ضرورت بکارگیری این سیستمها، با توجه به فضای ناامن حاکم بر شبکه های بزرگ و پیشرفتهایی که در روشهای حملات نفوذگران صورت پذیرفته است، به منظور تشخیص نفوذهای صورت گرفته و انجام اقدام مقتضی، اجتناب ناپذیر می باشد. این موارد نیاز به طراحی یک سیستم تشخیص نفوذ کارا و اثربخش را ضروری می نماید.

۱-۲ نوآوری طرح

تا کنون تلاشهای بسیاری برای اشتراک دانش بین سیستمهای تشخیص نفوذ صورت پذیرفته است. اما تحقیق موجود نسبت به کارهای قبلی متفاوت می باشد. در این طرح یک سیستم تشخیص نفوذ با انواع موتورهای با نظارت و بدون نظارت برای تهیه دانش ایجاد می نماییم که تهیه دانش در آن به صورت توزیع شده صورت می پذیرد. این نگاه به سیستمهای تشخیص نفوذ نگاهی متفاوت و جدید به شمار می آید. که نتایج ذیل را به همراه دارد:

أ. مبتنی بر مدل شبکه‌های اجتماعی

این اولین بار است که از مفهوم شبکه اجتماعی برای اشتراک دانش بین سیستمهای تشخیص نفوذ استفاده می شود. از آنجا که این مدل بر اساس معماری شبکه های اجتماعی بنا شده است. لذا به لحاظ زیرساختی محدودیتی در حوزه اجرا ندارد. یعنی هم می توان آنرا در یک شبکه محلی که در آن چندین سیستم تشخیص نفوذ وجود دارد، بکار برد. هم می توان در شبکه های بین چند سازمان آن را استفاده نمود. و حتی می توان آنرا در گستره وسیعی چون شبکه جهانی اینترنت مورد استفاده قرار داد.

ب. عدم محدودیت در نوع سیستم تشخیص نفوذ

اکثر مدلهای توزیع شده محدودیتهایی را در نوع و ساختار سیستمهای تشخیص نفوذی که قرار است دانش خود را به اشتراک گذارند، قایل شده اند. در این تحقیق با طراحی یک پروتکل ارتباطی و افزودن اجزایی به ساختار شبکه اجتماعی، این محدودیتها به حداقل رسانده شده است.

ج. استقلال کامل نودها(سیستمهای تشخیص نفوذ)

در این مدل، هر نود با عضویت در شبکه اجتماعی می تواند از دانش تولید شده توسط سایرین بهره مند شده و دانش خود را نیز با آنها به اشتراک گذارد. نقطه عطف در این طرح این است که چون هیچ کنترل کننده مرکزی وجود ندارد. لذا نودها در عین حالی که قادرند از دانش دیگران بهره مند شوند در همه موارد مربوط به یک سیستم تشخیص نفوذ کاملا مستقل بوده و صرف نظر از online یا offline بودن، قادر به انجام وظایف خود می باشند.

د. افزایش دامنه به اشتراک گذاری و متعاقبا بهبود کارایی

یکی از پیچیده ترین و پرهزینه ترین فرآیندها در یک سیستم تشخیص نفوذ، کسب دانش نفوذها است. سیستمهای تشخیص نفوذ مختلف با الگوریتم های متفاوتی برای افزایش توانمندی در این فرآیند، طراحی شده اند. بدیهی است هر چه بانک دانش یک سیستم تشخیص نفوذ گسترده باشد، قدرت تشخیص آن نیز افزایش پیدا خواهد کرد. در این تحقیق با گسترش دامنه اشتراک این امکان برای سیستمهای تشخیص نفوذ فراهم می شود تا بتوانند از دانشهای ایجاد شده توسط موتورهای مختلف که از الگوریتمهای متفاوتی استفاده می کنند بهره مند گردند.

در این پایان نامه، جنبه های تئوری و شبیه سازی یک شبکه اجتماعی از سیستم های تشخیص نفوذ مورد بررسی قرار گرفته است. این شبکه باعث گسترش پایگاه دانش[1] سیستم‌های تشخیص نفوذ عضو خواهد شد و توان بهره گیری از الگوریتم های مختلف را برای سیستم‌ها فراهم می نماید. جزئیات بیشتر در فصل‌های مختلف توضیح داده می شود.

[1] Knowledge Base

در فصل دوم به بررسی سیستم های تشخیص نفوذ از وجوه مختلف می پردازیم. در فصل سوم شبکه های اجتماعی را معرفی نموده و سرویس‌های مختلفی که از طریق این شبکه ها قابل عرضه است را بررسی می‌نماییم. در فصل چهارم مدل پیشنهادی معرفی می گردد. در فصل پنجم به معرفی سیستم‌های پایه‌ای که به منظور پیاده سازی مدل پیشنهادی استفاده شده‌اند می‌پردازیم. در فصل ششم با استفاده از شبیه سازی سیستم پیشنهادی با سیستم‌های موجود مقایسه می شود. و در فصل هفتم ضمن جمع بندی و نتیجه‌گیری، مسیر کارهای آتی نیز مشخص می گردد.

***

فصل دوم

سیستم‌های تشخیص نفوذ

در دهه گذشته، همراه با گسترش تکنولوژی اینترنت محیط جدیدی برای برنامه های کاربردی‌سیستم های کامپیوتری بوجود آمد. در همان زمان، برنامه های کاربردی شبکه های محلی و شبکه های گسترده در زمینه های تجارت، امنیت، صنعت و .... باعث وابستگی بیشتری به سیستم های کامپیوتری شد.

علاوه بر هک، موجودیت های جدیدی مانند کرم، اسب تراوا، ویروس و... باعث بوجود آمدن خطرات جدیدی برای جامعه کامپیوتر می شوند. با توجه به شرایط سیستم های کامپیوتری، قدرت دفاعی شبکه های کامپیوتری ضعیف می باشد. به هر حال، رشد شبکه های کامپیوتری، ارتباطات و وابستگی رو به رشد آن‌ها می‌تواند عواقب زیادی به دنبال داشته باشد. بنابراین امنیت یکی از شاخه های مهم تجاری و تحقیقاتی در سیستم های کامپیوتری می باشد.

خطرات ناشی از نفوذ به شبکه های کامپیوتری چیزی نیست که بر اساس تئوری احتمالات به آن توجه شود بلکه باید بصورت مداوم چک گردد، چون نفوذ ممکن است در هر لحظه رخ دهد. بعضی از گرایش های اخیر سیستم های تشخیص نفوذ در راستای تشخیص نفوذهای جدید می باشد.

یکی از نگرانی‌ها در زمینه تشخیص نفوذ، شناخت نفوذ و گزارش آن است که در این حالت سیستم تشخیص نفوذ، به سیستم تشخیص نفوذ و پاسخ تغییر پیدا می‌کند [Kab05]. یکی از مشکلات سیستم تشخیص نفوذ، تضمین برای شناختن نفوذ می باشد. این یکی از دلایلی است که سیستم تشخیص نفوذ بعنوان ابزار کمکی برای فرد خبره است زیرا سیستم تشخیص نفوذ قادر به تشخیص نفوذهای جدیدی که هیچ الگو[1] یا دانشی در

[1] Signature

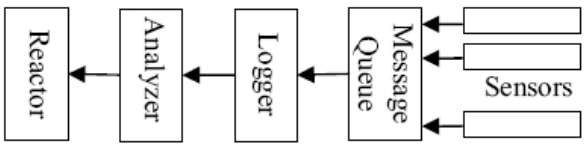
مورد آن‌ها نداشته باشد نمی باشد. اگر چه روش‌های جدید باعث بهبود در این دیدگاه شده اند ولی هنوز در این زمینه راه زیادی باقی است.

۲-۱ مطالعه سیستمهای تشخیص نفوذ

در این بخش به منظور آشنایی با انواع سیستمهای تشخیص نفوذ به بررسی آنها از زوایای مختلف می پردازیم.

۲-۱-۱ معماری سیستم‌های تشخیص نفوذ

معماری های سیستم‌های تشخیص نفوذ[1] خیلی متنوع و گوناگون است. محققین به منظور جمع آوری داده‌ها، تحلیل، و پاسخگویی در کل حیطه متمرکز، نامتمرکز، تعاملی و مستقل اجزایی کلیدی را برای این سیستم ها پیاده سازی کرده اند. در حال حاضر سیستم های تشخیص نفوذ، در گستره ای از سیستم‌های مبتنی بر میزبان شخصی، که جمع آوری و تحلیل کلیه داده‌ها در آن‌ها به صورت محلی صورت می گیرد، تا سیستم‌های مبتنی بر شبکه یا حتی سیستم‌های تعاملی توزیع شده بین چندین سازمان، که جمع آوری داده و تحلیل و پاسخگویی را هم به صورت محلی و هم توزیع شده انجام می دهند، قرار دارند. اگرچه این سیستم ها نیازمندی‌های متفاوتی دارند، اما به لحاظ عملکرد از یکسری اجزای مطابق شکل ۲-۱ مشخص تشکیل شده اند [Don04]. برای مثال می توان از سیستم‌های [Mic07, Wan04] به عنوان سیستم‌هایی که عملکرد آن‌ها مبتنی بر میزبان است و سیستم‌هایی مانند [Jev96, Dfr00, Pap97] که سیستم‌هایی توزیع شده و تعاملی می باشند نام برد.



شکل ۲-۱: اجزای اصلی یک سیستم تشخیص نفوذ [Pre04]

[1] Intrusion Detection System (IDS)

أ. **حسگر**: این جزء نقش نظارت بر ترافیک تحت پوشش را دارد و می تواند به صورت متمرکز و یا توزیع شده در شبکه قرار گیرد و وظیفه آن جمع آوری داده های لازم برای موتور[۱] سیستم تشخیص نفوذ می باشد. این داده‌ها بسته به نوع سیستم تشخیص نفوذ و روش بکار رفته در موتور آن می تواند کلیه بسته‌های[۲] ارسالی، بخشی از آن‌ها و یا حتی بخشی از محتوای آن‌ها باشد.

ب. **صف پیام**[۳]: اطلاعات جمع آوری شده توسط حسگرها از طریق یک کانال ارتباطی به واقعه‌نگار ارسال می‌شود. این کانال بسته به ساختار حسگرها و معماری سیستم تشخیص نفوذ ممکن است بستر شبکه، یا یک لایه برنامه کاربردی[۴] باشد. در هر صورت به دلیل حجم بالای اطلاعات ارسالی از حسگرها نیاز به یک بافر واسط جهت ذخیره سازی موقت آن‌ها و تحویل به واقعه‌نگار در زمان مناسب می باشد. صف پیام نقش این بافر را ایفا می نماید.

ج. **واقعه‌نگار:** این جز نیز بسته به معماری سیستم تشخیص نفوذ ممکن است اصلا وجود نداشته باشد (مانند نمونه هایی که از On the fly processing استفاده می کنند). اما در اکثر روش‌ها این جزء یک بخش ضروری از معماری به شمار آمده و وظیفه آن نگهداشت کلیه اطلاعات جمع آوری شده توسط حسگرها در ساختار مناسب و قابل استفاده توسط تحلیلگر می باشد. ساختار این جزء نیز بسته به تکنیک استفاده شده در تحلیلگر متفاوت بوده و ممکن است فایل، پایگاه داده یا ... باشد.

د. **تحلیلگر:** شاید بتوان تحلیلگر را اصلی ترین جزء سیستم تشخیص نفوذ به شمار آورد. زیرا که پردازش و تحلیل داده ها به منظور تشخیص نفوذهای احتمالی در این جزء صورت می پذیرد. بسته به نوع رویکرد بکارگرفته شده در سیستم تشخیص نفوذ، مکانیسم ها (تکنیک های) مختلفی برای پردازش داده ها به خدمت گرفته می‌شوند[Prez04].

---

[1] Engine

[2] Packet

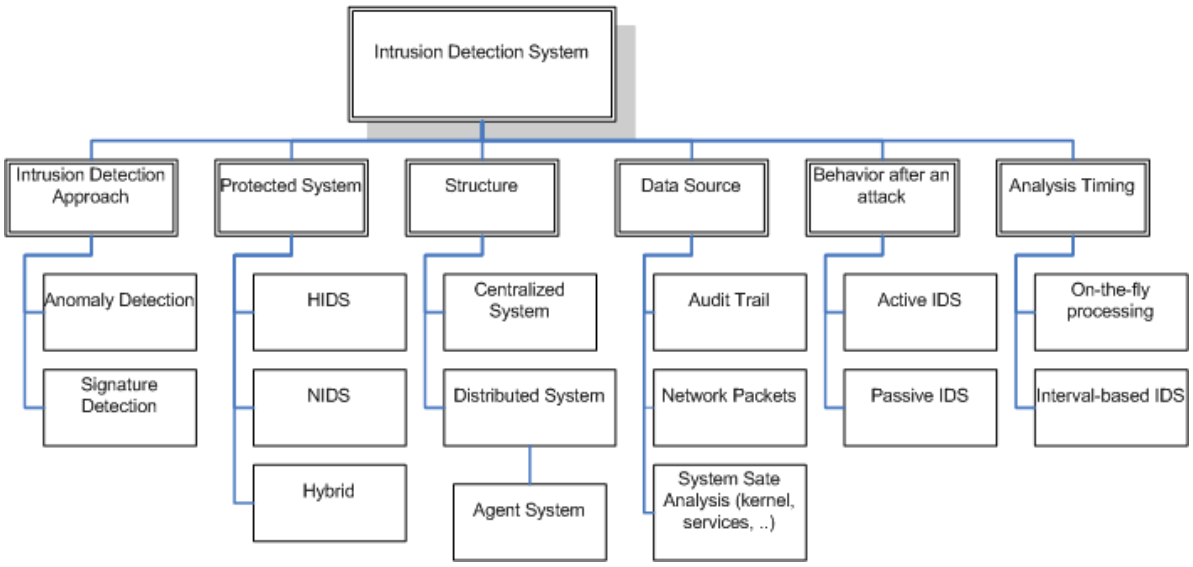
[3] Message Queue

[4] Application

ه. **واکنشگر**[1]: بعد از تشخیص نفوذ توسط تحلیلگر، نوبت به این جزء جهت انجام اقدام مناسب می باشد. بسته به نوع سیستم تشخیص نفوذ (فعال یا غیرفعال) این اقدام می تواند متفاوت باشد. در سیستم‌های فعال که در رده سیستم جلوگیری از نفوذها[2] دسته بندی می شوند، با قطع ارتباط در مقابل نفوذ تشخیص داده شده عکس العمل نشان می دهند. اما در سیسمتم های غیرفعال صرفا به اعلان هشدار کفایت می‌کنند.

۲-۱-۲ طبقه بندی سیستم‌های تشخیص نفوذ

سیستم‌های تشخیص نفوذ را می توان از دیدگاه های مختلفی طبقه بندی نمود. در شکل ۲-۲[Pre04] از وجوه مختلف دسته بندی صورت گرفته است.



شکل ۲-۲: طبقه بندی سیستم‌های سیستم تشخیص نفوذ

أ. **رویکرد**[3]

- تشخیص رفتار[4]: با مدل کردن یک الگوی رفتاری نرمال، و نظارت بر الگوهای رفتاری دیگر موارد نفوذ تشخیص داده می شود.[Kab05]

[1] Reactor
[2] Intrusion Prevention System(IPS)
[3] Approach
[4] Anomaly Detection