جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

Archvie of SID

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

سیستم تشخیص نفوذ مبتنی بر شبکه اجتماعی(SNIDS)

مهدی علیزاده ثانی[۱]، عباس قائمی بافقی[۲]

[۱]دانشگاه پیام نور تهران
m.alizadeh@gmail.com
[۲]دانشگاه فردوسی مشهد
ghaemiB@um.ac.ir

چکیده

در این مقاله با ترکیب سیستم‌های تشخیص نفوذ با شبکه اجتماعی معماری جدیدی ارایه گردیده، که در آن برای سیستم‌های تشخیص نفوذ در بستر شبکه اجتماعی امکان اشتراک دانش فراهم شده است. این سیستم از یک دیدگاه در رسته سیستم‌های توزیع شده قرار می‌گیرد. اما به لحاظ عملکردی کاملا با آنها متفاوت می‌باشد. عمده‌ترین تفاوت آن در نحوه کسب دانش‌های جدید است. سیستم پیشنهادی که SNIDS نامگذاری گردیده است، بر مشکلاتی نظیر عدم توسعه‌پذیری، وجود نقطه شکست و محدودیت در نوع سیستم تشخیص نفوذ فایق می‌آید.

ابتدا با ارایه یک معماری توزیع شده مبتنی بر ساختار شبکه اجتماعی و قراردادن سیستم‌های تشخیص نفوذ به عنوان گره‌های 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 نام‌های Snort[۱] و Bro[۲] توسعه داده شده است. نتایج ارزیابی اولیه با استفاده از داده‌های DARPA2000[۳] بر روی این سیستم نشان دهنده تاثیر اشتراک دانش در بهبود عملکرد سیستم‌های تشخیص نفود می‌باشد. به گونه‌ای که دقت تشخیص SNIDS به نسبت سیستم‌های پایه ۱۸% بهبود داده شده است.

واژه‌های کلیدی

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

۱- مقدمه

با رشد سریع اینترنت تنش‌های مربوط به آن نیز افزایش یافته است. علاوه براین تکنولوژی نفوذ به سمت روش‌های پیچیده ای نظیر حملات هماهنگ و مشارکتی سوق پیداکرده است. در چنین شرایطی نیاز مبرم به ابزارهای نرم افزاری که بتوانند به صورت خودکار دامنه وسیعتری از نفوذها را شناسایی کنند، احساس می شود. سیستم‌های تشخیص نفوذ به عنوان نگهبان شبکه باید توانایی شناسایی و دفاع را در زمان بسیار کوتاه داشته باشند.

معماری‌های سیستم‌های تشخیص نفوذ بسیار متنوع و گوناگون است. اگرچه این سیستم‌ها نیازمندی‌های متفاوتی دارند، اما به لحاظ عملکرد از یکسری اجزای مشخص تشکیل شده اند و در همه آنها اجزاء اصلی جمع آوری و تحلیل داده‌ها وجود دارد. در حال حاضر سیستم‌های تشخیص نفوذ، در گستره‌ای از سیستم‌های مبتنی بر میزبان شخصی تا سیستم‌های مبتنی بر شبکه یا حتی سیستم‌های تعاملی توزیع شده بین چندین سازمان قرار دارند.

در یک دسته بندی کلی، می‌توان سیستم‌های تشخیص نفوذ را به سیستم‌های متمرکز و سیستم‌های توزیع شده تقسیم بندی نمود. در سیستم‌های متمرکز تمام اجزای سیستم تشخیص نفوذ به صورت یکجا و بر روی یک رسانه در شبکه فعالیت می‌کنند. اما در سیستم‌های توزیع شده با هدف افزایش ضریب ایمنی، حمل‌پذیری آسیب و توزیع بار ترافیکی شبکه تمام یا برخی از اجزای سیستم تشخیص نفوذ مانند حسگرها، واقعه نگار و یا حتی جزء تحلیلگر بر روی ناحیه‌های مختلف یک شبکه یا چندین شبکه متفاوت توزیع می‌شوند. در سیستم‌های توزیع شده موجود نظیر GrIDS[۶]، DIDS[۵]، EMERALD[۴] و AAFID[۷] یا سیستم‌های مبتنی بر عاملهای متحرک[۸]، جزء تحلیلگر بین بخشهای مختلف شبکه توزیع شده است. همچنین در سیستم‌های توزیع شده دیگری نظیر

جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

Archive of SID

TaoPeng[۹] جزء حسگر و یا در سیستم معرفی شده در [۱۰] جزء واقعه نگار(Logger) بین بخش‌های مختلف شبکه توزیع شده است. اما در هیچیک از این سیستم‌ها جزء استنتاج دانش توزیع نشده است.

رویکردهای بکارگرفته شده در سیستم‌های تشخیص نفوذ را می‌توان به دو دسته کلی مبتنی بر رفتار و مبتنی بر امضاء تقسیم بندی نمود. رویکرد مبتنی بر رفتار، با مدل کردن یک الگوی رفتاری نرمال و نظارت بر الگوهای رفتاری دیگر موارد نفوذ تشخیص داده می‌شود. و رویکرد مبتنی بر امضاء با نگهداری یک پایگاه داده از امضاءهای نفوذهای شناخته شده، موارد مطابق شده با آنها به عنوان نفوذ شناخته می‌شوند.

کارهای انجام شده در بیشتر سیستم‌های تشخیص نفوذ با هدف بهبود کارایی و کارآمدی بخش تحلیلگر در این سیستم‌ها صورت گرفته است. روش دیگر بهبود کارآمدی سیستم تشخیص نفوذ با افزایش دامنه تشخیص و گسترش پایگاه دانش حاصل می شود. تلاش‌ها و تحقیقات صورت گرفته در زمینه بهبود کارآمدی در سیستم‌های تشخیص نفوذ، هر کدام باعث بهبود بخشی از عملکرد این سیستم‌ها گردیده است، ولی هیچ کدام از این تکنیک‌ها یا معماری‌ها نمی‌تواند به تنهایی انواع حملات در شبکه عظیمی مانند اینترنت را تشخیص دهد. لذا موضوع تعامل و اشتراک اطلاعات بین این سیستم‌ها که هر کدام تکنیک و معماری خاص خود را دارند می‌تواند باعث افزایش قدرت تشخیص آنها از طریق گسترش پایگاه دانش باشد.

شالوده‌ای که در اینجا به عنوان بستر تعاملی برای سیستم‌های تشخیص نفوذ مورد استفاده قرار گرفته است، شبکه اجتماعی می‌باشد. شبکه اجتماعی در یک بیان کلی یک ساختار اجتماعی ایجاد شده توسط گره‌هایی است (که هر کدام مستقل هستند) که بوسیله نوع خاصی از وابستگی متقابل مانند اطلاعات، دیدگاه، عقیده، تعاملات مالی، دوستی، خویشاوندی، تجارت و ... به هم پیوسته شده اند. در این مقاله یک معماری توزیع شده با رویکرد مبتنی بر امضاء ارایه شده و با بکارگیری شبکه اجتماعی و قراردادن سیستم‌های تشخیص نفوذ به عنوان گره‌های این شبکه و تعریف پروتکل و ساختار ارتباطی، امکان اشتراک دانش بین سیستم‌های تشخیص نفوذ فراهم آمده است.

سیستم پیشنهادی در واقع به عنوان یک مکمل می‌تواند در کنار هر یک از این نوع سیستم‌ها قرار گیرد و امکان اشتراک دانش‌های جدید را بین سیستم‌های تشخیص نفوذ فراهم نماید. به عبارت دیگر سیستم پیشنهادی فراتر از سطح سیستم‌های تشخیص نفوذ بوده و برای ایجاد ارتباط بین آنها بکار می‌رود.

مزایایی بکارگیری این سیستم در کنار سیستم‌های موجود شامل: گسترش پایگاه دانش تشخیص، بهره‌گیری از الگوریتم‌های متفاوت در استنتاج دانشهای جدید، حذف نقطه شکست، قابلیت توسعه‌پذیری نامحدود و امکان بهره‌گیری از سیستم‌های تشخیص نفوذ ناهمگون می‌باشد.

در بخش دوم این مقاله به بررسی کارهای مرتبط با اشتراک دانش در سیستم‌های تشخیص نفوذ و در بخش سوم به تشریح سیستم پیشنهادی و اجزای مختلف آن می‌پردازیم. در بخش چهارم به مقایسه سیستم پیشنهادی و سیستم‌های مشابه پرداخته و نتایج ارزیابی اولیه سیستم SNIDS را ارایه می‌نماییم.

۲-کارهای مرتبط

کارهای انجام شده در رابطه با سیستم‌های تشخیص نفوذ در حوزه اشتراک دانش، که با عناوین مختلفی نظیر سیستم‌های توزیع شده تعاملی، سیستم‌های توزیع شده، اشتراک اطلاعات و دیگر عناوین نام برده شده است، را بررسی می‌کنیم:

Tao Peng و همکارانش مقاله ای با عنوان "مدل اشتراک برای سیستم‌های توزیع شده[۹]" را ارایه نموده اند. در این مدل آمارها توسط یک الگوریتم جمع تراکمی گردآوری می‌شود. سپس با استفاده از یک رویکرد یادگیری ماشین به هماهنگ سازی اطلاعات به اشتراک گذاشته شده در بین سیستم‌های تشخیص توزیع شده پرداخته می‌شود.

بزرگترین اشکال این مدل وجود هماهنگ‌ساز (به عنوان یک ابزار متمرکز) است که علاوه بر گلوگاه شدن، امکان Single Point Failed وجود خواهد داشت. همچنین آسیب پذیری مدل نیز به دلیل وجود هماهنگ ساز افزایش می‌یابد. در مقابل سیستم SNIDS فاقد هر گونه کنترل کننده مرکزی است و در آن هر سیستم تشخیص نفوذ به تنهایی و به صورت محلی در خصوص نفوذها تصمیم گیری و از شبکه اجتماعی ایجاد شده برای اشتراک دانش با دوستان استفاده می‌نماید.

در[۱۰] برای یکپارچه سازی سیستم‌های تشخیص نفوذ همگون و ناهمگون دو مدل ارایه شده است. در مدل یکپارچه سازی مستقیم با استفاده از یک کنسول واحد، مدیریت و نظارت چندین سیستم صورت می‌گیرد. بدین ترتیب سیستم‌ها می‌توانند داده‌هایشان را متقابلا به اشتراک گذارند. اما در یکپارچه سازی غیرمستقیم که با استفاده از یک نرم افزار مدیریت رخدادها و اطلاعات امنیتی (SIEM) انجام می‌شود، روش به این صورت است که اطلاعات از logهای مختلف جمع آوری می‌شود و از طریق SIEM همبستگی و هماهنگی بین آنها انجام می‌شود.

در مدل اول هر چند که نقش کنسول مدیریتی کم رنگتر است، اما وجود آن به عنوان یک ناظر می‌تواند مشکل تمرکز سرویس را بوجود آورد که در معرض آسیب‌پذیری‌های بیشتری می‌باشد. معضل دیگر که توسط نویسندگان نیز مطرح گردیده عدم همکاری برخی سیستم‌ها در اشتراک اطلاعات می‌باشد. در مورد مدل دوم همچنان مشکلات مطرح شده در [۹] وجود دارد. در صورتی که در

جهت تهیه فایل WORD این مقاله به سایت DaneshResan.com مراجعه نمایید و عنوان مقاله را جستجو کنید
بیش از ۲ میلیون مقاله فارسی در این سایت موجود میباشد

Archvie of SID

SNIDS عملا هیچ گرهی وظیفه هماهنگ‌سازی را بر عهده نداشته و محدودیتی نیز در نوع سیستم تشخیص نفوذ وجود ندارد.

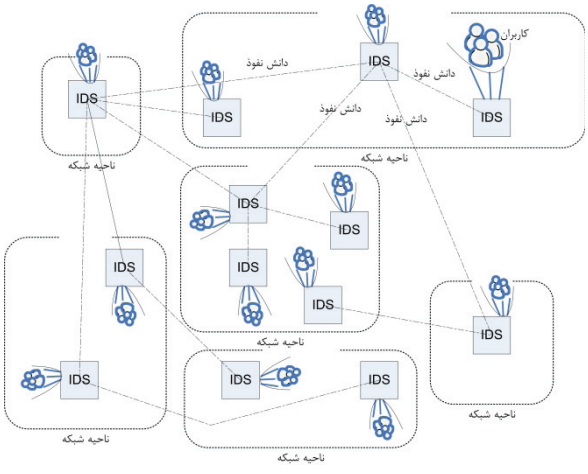
Geetha, Delbert یک سیستم تشخیص نفوذ غیر متمرکز معرفی نموده اند[۱۱]. یک شبکه همسایگی مجازی که در آن هر همسایه وظیفه مراقبت از دیگری به عهده دارد. با مشاهده یک نفوذ، دیگران نیز مطلع شده و فیدبک لازم از آنها جمع آوری می شود. هر سایت عامل‌های متحرکی را در دوره‌های زمانی مشخصی برای بررسی همسایه‌ها و ارایه گزارش اعزام می‌نماید.

در این مدل هر چند که هیچ کنترل کننده مرکزی وجود ندارد اما تفاوت‌های آن با شبکه اجتماعی مطرح شده دو مورد است. اولا در روش واکنش در مقابل نفوذ که در این مدل با جمع آوری فیدبک‌ها عملا نتیجه گیری با رای گیری انجام می‌شود. اگر چه که کسب نتیجه صحیح تر خواهد بود اما سرعت آنالیز نیز به همان نسبت کاهش می‌یابد. دوما در این مدل هیچ اشتراک دانشی صورت نمی‌گیرد و هر سیستم به تنهایی به جمع‌آوری دانش در باره نفوذها پرداخته و فقط برای تصمیم گیری از کمک سایرین استفاده می‌نماید.

۳- معرفی سیستم پیشنهادی

یکی از روش‌های نوین اشتراک دانش، استفاده از الگوی شبکه‌های اجتماعی است. چنانکه از نام سیستم SNIDS نیز برمی آید، سیستمی است مبتنی بر شبکه اجتماعی و ماهیت عملکردی آن یک روش مبتنی بر همکاری می‌باشد.

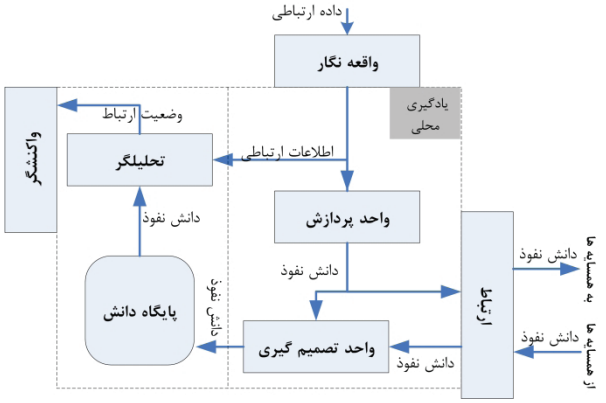
نمای کلی SNIDS مطابق شکل (۱) است. همانطور که در این شکل نیز نشان داده شده قالب کلی شبکه اجتماعی حفظ گردیده اما به منظور فراهم نمودن امکان اشتراک دانش نفوذ بین سیستم‌های تشخیص نفوذ، تغییر داده شده و سیستم‌های تشخیص نفوذ به همراه کاربران خود، جایگزین نودهای انسانی گردیده اند. همچنین این شبکه همانند هر شبکه سراسری دیگر از تعدادی ناحیه تشکیل شده است. در ادامه به تشریح اجزای سیستم و روابط بین آنها می‌پردازیم.



شکل ۱: نمای کلی سیستم SNIDS

۳-۱ گره (سیستم تشخیص نفوذ)

شکل (۲) یک نمای شماتیک توسعه داده شده از سیستم تشخیص نفوذ است و اجزای لازم برای هر گره نمایش داده شده است. از آنجا که اجزای کلی بین تمام سیستم‌های تشخیص نفوذ مشابه می‌باشند، صرفا به تشریح بخش‌های موثر در سیستم پیشنهادی می‌پردازیم.



شکل ۲: اجزای سیستم تشخیص نفوذ به عنوان یک گره در شبکه اجتماعی

الف) جزء ارتباط: این جزء وظیفه تبادل دانش با دیگر گره‌ها در شبکه اجتماعی را بر عهده دارد. پروتکل تبادل دانش نیز در همین جزء استقرار دارد. دانشی که توسط گره‌های دیگر منتشر می‌شود توسط این جزء دریافت و سپس عمل نگاشت از قالب پروتکل به قالب داخلی صورت می‌گیرد که نتیجه حاصل دانشی قابل درک توسط سیستم تشخیص نفوذ محلی می‌باشد. این دانش به واحد تصمیم گیری از جزء یادگیر محلی تحویل داده می‌شود و این جزء پس از دریافت دانش از واحد استنتاج دانش محلی هماهنگی لازم جهت تبدیل دانش از قالب داخلی به قالب پروتکل را صورت داده و آن را منتشر می‌نماید.

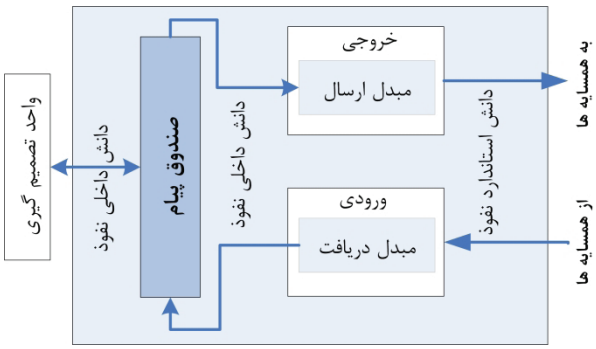
ب) یادگیر محلی: در سیستم‌های تشخیص نفوذ یادگیر الگوهای جدید نفوذ شناسایی و به پایگاه دانش اضافه می‌گردد. این وظیفه در سیستم SNIDS توسط جزء یادگیر محلی انجام می‌شود. این جزء شامل دو واحد پردازش و تصمیم گیری می‌باشد. واحد پردازش وظیفه تحلیل اطلاعات جمع آوری شده در واقعه نگار را برای کشف الگوهای جدید بر عهده دارد. الگوهای کشف شده با کمک واحد تصمیم گیری به پایگاه دانش اضافه می‌شود. واحد تصمیم گیری علاوه بر دریافت ورودی از واحد پردازش به عنوان یک موتور تولید کننده دانش محلی، دانش مربوط به نفوذهای شناخته شده را نیز از واحد ارتباط، که دانش به اشتراک گذاشته شده توسط دیگر سیستم‌های تشخیص نفوذ موجود در شبکه را گردآوری می‌کند، دریافت می‌نماید. همچنین این واحد در رابطه با چگونگی افزودن دانش اخذ شده به پایگاه دانش تصمیم گیری می‌نماید که در صورت نیاز، دانش جدید به پایگاه دانش افزوده و

Archive of SID

مبنای عملکرد تحلیلگر قرار می‌گیرد. از طرف دیگر این واحد پس از تصمیم گیری در مورد کشف دانش جدید، آن‌ها را همزمان با افزودن به پایگاه دانش محلی به جزء ارتباط نیز جهت انتشار تحویل می‌دهد.

۳-۲ پروتکل ارتباط با همسایگان

جهت ارتباط سیستم‌های تشخیص نفوذ مختلف در سیستم پیشنهادی یک قالب استاندارد معرفی می‌شود. در واحد ارتباط دانش عمل نگاشت دانش از قالب موجود در سیستم تشخیص نفوذ به قالب استاندارد شبکه و بالعکس صورت می‌پذیرد. همانطور که در شکل (۳) نمایش داده شده است، این جزء از سه قسمت اصلی واحد ورودی، واحد خروجی و صندوق پیام تشکیل گردیده است.



شکل ۳: اجزای داخلی جزء مبادله کننده دانش

الف) واحد ورودی: داده‌ها توسط واحد ورودی که منتظر پیام‌های یک پروتکل خاص از یک آدرس ویژه در شبکه اجتماعی می باشند، دریافت می‌شوند. پیام بعد از دریافت به تطبیق دهنده (مبدل) ارسال می‌شود. پیام دریافتی، که به قالب استاندارد شبکه ارسال شده به یک پیام با قالب سیستم تشخیص نفوذ محلی تبدیل می‌گردد و اطلاعات توصیفی مناسب به نقطه‌ی پایانی اطلاعات دریافت شده اضافه می‌شود و در نهایت پیام به صندوق پیام انتقال می‌یابد.

ب)صندوق پیام: صندوق پیام یک جزء همواره فعال است و کلیه پیامهای ارسالی و دریافتی در آن ذخیره می‌شوند. صندوق پیام، پیامهای جدید را برای مبدل ارسال در واحد خروجی می‌فرستد.

ج) واحد خروجی: در واحد خروجی مبدل ارسال قرار دارد. در این مبدل تبدیل پیام از قالب محلی به قالب استاندارد شبکه انجام می‌شود و سپس از طریق پورت توافق شده برای سایر گره‌های دوست (سیستم‌های تشخیص نفوذ) ارسال می‌گردد.

شکل کلی قالب پیام جهت مبادله دانش نفوذهای شناخته شده مطابق زیر است. این قالب از الگوی ارایه شده در [۱۲] جهت پیکربندی امضاهای سیستم‌های تشخیص نفوذ در کنترل کننده بیسیم سیسکو، اقتباس شده است. هدف از مشخصات توصیفی که همراه الگوهای امضاء ارسال می‌شوند، ارایه اطلاعات تکمیلی در مورد وضعیت، شرایط و عملی است که سیستم تولید کننده پیام در رابطه با این امضاء داشته است. این اطلاعات سیستم مقصد را در تصمیم گیری راهنمایی می‌نماید.

```
<?xml version="1.0" encoding="utf-8"?>
<SignaturePattern
xmlns="http://www.ids.com/social/signature" >
<signuature ids="" name="" version="" precedence=""
frequency="" interval="" quiet="" action="" desc="">
<patterns>
<pattern>pattern 1 context</pattern>
<pattern>pattern 2 context</pattern>
<pattern>pattern N context</pattern>
</patterns>
</signuature>
</SignaturePattern>
```

name : نام امضاء، توسط این رشته یک امضاء معرفی می‌شود.

ids: نام سیستم تشخیص نفوذ در شبکه اجتماعی، این رشته بایستی یک نام منحصر به فرد باشد. نام کامل امضاء ترکیب نام سیستم تشخیص نفوذ و نام امضاء خواهد بود

precedence : اولویت امضاء، یک عدد که نشان دهنده اولویت جایگاه امضاء در پایگاه دانش است.

pattern : الگوی امضاء، مقدار نشانه ذخیره شده در این پارامتر، برای انطباق با بسته‌های شبکه استفاده می‌شود. حداقل یک الگو برای هر امضاء الزامی است. برای الگوی امضاء، از قالب تعریف شده در سیستم Snort بهره گرفته شده است. که در آن هر امضاء شامل دو بخش منطقی اصلی به نام "سرآیند" و "گزینه‌ها" می‌باشد. بخش اول شامل اطلاعاتی است که تعیین می‌کند آن امضاء، موارد مشکوک مربوط به کدام شبکه، کدام محل و چه نوع بسته‌ای را باید مورد بررسی قرار داده و چه عملی را باید در مقابل این حرکت مشکوک انجام دهد. بخش دوم شامل گزینه‌های متنوع برای کشف مزاحمت در شبکه و اعلام هشدار است.

frequency: تعداد بسته‌های منطبق در بازه اندازه گیری. مقدار این نشانه مشخص می‌کند که چند تا بسته در مدت اندازه‌گیری، بایستی با این الگو منطبق شوند تا action امضاء اجرا گردد. مقدار صفر به معنای این خواهد بود که به محض تطابق یک بسته با الگو، بایستی عمل مناسب اجرا گردد.

interval: بازه اندازه‌گیری به ثانیه. مقدار این نشانه تناوب زمانی برای انطباق frequency را مشخص می‌کند. مقدار پیش فرض این نشانه ۱ ثانیه می‌باشد.

quiet : زمان صبر به ثانیه، مقدار این نشانه مشخص کننده مدت زمانی است که حسگرها هیچ بسته منطبق بر امضاء را دریافت نمی کنند. بدین شکل می‌توان نتیجه گیری کرد که حمله با این

Archvie of SID

امضاء فروکش کرده است. مقدار صفر نشانه frequency باعث نادیده گرفتن این نشانه خواهد شد.

action: واکنش. عملی را که سیستم تشخیص نفوذ بایستی در صورت تطابق امضاء انجام دهد، مشخص می‌نماید. این عمل یکی از مقادیر none یا report خواهد بود.

desc: توضیح درباره امضاء. این عبارت هدف از امضاء را مشخص می‌نماید.

۳-۳ سرویس شبکه اجتماعی

در این بخش به توصیف سرویس شبکه اجتماعی که به عنوان بستر اشتراک دانش در این تحقیق در نظر گرفته شده است می‌پردازیم.

الف) عضویت

برای عضویت در شبکه، ابتدا بایستی سیستم تشخیص نفوذ به صورت داخلی توسعه داده شود تا قابلیت به اشتراک گذاری دانش خود را با سایرین داشته باشد. بعد از انجام توسعه‌های داخلی، می‌تواند با دریافت دعوتنامه از سایر سیستم‌های عضو شبکه به عضویت آن درآید. و اگر به صورت مستقل و بدون دعوتنامه بخواهد عضو شبکه شود این کار با ارسال اطلاعاتی اولیه به سرور شبکه اجتماعی ممکن خواهد شد.

توجه داشته باشید که سرور مرکزی هیچ مسئولیت در رابطه با کیفیت عملکرد سیستم‌های عضو ندارد. مگر اینکه از نود خاصی شکایت شود و یا قوانین شبکه توسط سیستمی نقض گردد. تمام سیستم‌ها در هنگام عضویت بایستی قوانین شبکه را بپذیرند.

بدین ترتیب بعد از تایید سرور مرکزی و پذیرش قوانین شبکه توسط درخواست دهنده، عضویت صورت می‌پذیرد و به سیستم یک شناسه منحصر به فرد که در مدل پیشنهادی آدرس شبکه ای است که سیستم تشخیص نفوذ از آن حفاظت می‌کند، اختصاص می‌یابد.

ب) پروفایل

ایجاد پروفایل معمولا همزمان با فرآیند عضویت صورت می‌پذیرد. هر سیستم موظف به ارایه اطلاعاتی در مورد ویژگی‌ها و ساختار خود می‌باشد. این اطلاعات دارای رده‌های دسترسی متداول در سرویس‌های شبکه اجتماعی می‌باشد (عمومی، در دسترس دوستان، شخصی). هدف از این اطلاعات امکان شناسایی سیستم توسط نودهای دیگر و احیانا برقرای رابطه دوستی می‌باشد.

اطلاعاتی نظیر آدرس میزبان سیستم تشخیص نفوذ، شهر، کشور، تاریخ شروع فعالیت در وب، معماری سیستم تشخیص نفوذ، میزان خطر در شبکه، محلی بودن شبکه، تعداد سیستم‌های تشخیص نفوذ فعال در شبکه، از جمله فیلدهایی است که به عنوان پروفایل یک سیستم تشخیص نفوذ در سرویس شبکه اجتماعی نگهداری می‌شود.

پ) دوستیابی

بعد از عضویت و تکمیل پروفایل، اقدام بعدی انتخاب دوستانی به منظور اشتراک دانش با آنها می‌باشد. به محض عضویت در سیستم و تکمیل پروفایل، سرویس شبکه بر اساس اطلاعات پروفایل اقدام به جستجوی موارد مشابه کرده و نودهایی را برای دوستی پیشنهاد می‌دهد. اگر هم دوستانی داشته باشید و یا از کانال دوستی به عضویت شبکه درآمده باشید، دوستان دوست شما نیز به شما پیشنهاد می‌شوند.

برای پیدا کردن نودهایی با مشخصات خاص، می‌توان جستجو کرد و مواردی مانند تعداد دوستان، نظرات دیگران و ... نیز در اولویت بندی نتایج جستجو تاثیرگذار خواهند بود.

در نهایت سیستم به نحوی نودها را شناسایی و به آنها پیشنهاد دوستی می‌دهد. پیشنهاد مطرح شده به سیستم طرف مقابل اعلام می‌گردد و او نیز با بررسی پروفایل پیشنهاد دهنده آن را پذیرفته یا رد می‌کند. بدین ترتیب ساختار اجتماعی شبکه شکل می‌گیرد.

ت) هوادار

سیستم‌های تشخیص نفوذی که خارج از دنیای مجازی سرویس شبکه اجتماعی، دارای اعتبار جهانی هستند، معمولا تعداد زیادی پیشنهاد دوستی دریافت می‌کنند. از آنجا که ارزیابی همه پیشنهادات نیازمند صرف زمان و هزینه است. لذا این نودها امکان دوستی‌های یکطرفه (هوادار) را فراهم می‌کنند. بدین ترتیب این سیستم‌ها می‌توانند دانش خود را برای همه هواداران قابل استفاده نمایند. اما غیر از دوستانشان از دیگران دانشی را نمی‌پذیرند.

۴-۳ شیوه‌های تبادل دانش در شبکه

بعد از ایجاد شبکه از طریق مکانیسم‌های دوستیابی مطرح شده در بخشهای قبلی، نوبت به اشتراک دانش می‌رسد. در اینجا به ارایه شیوه‌هایی برای انتقال دانش بین نودها می‌پردازیم.

الف) ارسال بدون اجازه

در این روش، هر نود به محض دوست شدن با یک نود دیگر، تمام دانش خود را بر اساس پروتکل شبکه برای او ارسال می‌نماید. البته نود مقصد هیچ الزامی در بررسی یکباره تمام دانش‌های موجود در صندوق پیام خود را ندارد و می‌تواند این کار در چند مرحله انجام دهد.

ارسال همه دانش: بعد از ایجاد رابطه دوستی بین دو نود و در صورتی که از شیوه "ارسال بدون اجازه" استفاده شده باشد، هر نود می‌تواند تمام دانش موجود در پایگاه دانش خود را که هنوز برای دوست جدیدش ارسال نکرده به یکباره برای او ارسال نماید.

Archive of SID

ارسال بخش به بخش: در این شیوه، سرویس ارسال کننده دانش، به صورت چرخشی پایگاه دانش محلی را پیمایش می‌نماید و در هر نوبت تعدادی از دانش‌های موجود در پایگاه دانش را برداشته و برای تمامی دوستانی که تا کنون این دانش‌ها برای آن‌ها ارسال نشده است، ارسال می‌نماید.

ب) برداشت انتخابی

در این روش، هر نود پس از تکمیل عضویت در شبکه، تمام دانش خود را به فرمت استاندارد شبکه تبدیل کرده و سطح دسترسی آن را "قابل دسترس توسط دوستان" تعریف می‌نماید. سپس به اقدام به دوستیابی و تشکیل شبکه می‌دهد. دوستان می‌توانند به بررسی دانش به اشتراک گذاشته شده پرداخته و در صورت تمایل برخی از آنها را انتخاب و به پایگاه دانش محلی خود انتقال دهند.

۳-۵ مکانیزم بهنگام‌سازی پایگاه دانش محلی

در سیستم SNIDS، هر سیستم تشخیص نفوذ بر مبنای تعاریف و روشهای معمول در شبکه‌های اجتماعی و از طریق ارسال پیام، پایگاه قوانین خود را با دیگر سیستم‌های تشخیص نفوذ به اشتراک می‌گذارد. بدین صورت هر بار با اضافه شدن یک دانش جدید به پایگاه دانش، آن را از طریق جزء مبادله کننده دانش به قالب استاندارد معماری تبدیل می‌کند و برای دیگر دوستان خود ارسال می‌نماید. آنها نیز با بررسی صندوق پیام خود متوجه دریافت دانش جدید می‌شوند. این دانش از طریق جزء ارتباط به قالب محلی تبدیل شده و به سیستم تشخیص نفوذ وارد می‌شود. و بخش تصمیم گیری از واحد یادگیری محلی در مورد آن تعیین تکلیف می‌نماید. در صورت تایید، این بخش دانش در پایگاه داده اضافه می‌شود. البته این گره نیز صرف نظر از پذیرش یا عدم پذیرش دانش آن را برای دیگر دوستان خود ارسال می‌نماید. برای جلوگیری از وقوع حلقه، هر گره برای هر دانش فقط یکبار عمل ارسال را انجام می‌دهد. بدین ترتیب هر دانش جدید که بوجود می‌آید از طریق این شبکه اجتماعی با دیگر سیستم‌ها به اشتراک گذاشته می‌شود.

۴- ارزیابی و مقایسه

سیستم SNIDS را به دو صورت مورد ارزیابی قرار داده‌ایم. ابتدا ویژگی‌های سیستمی آن را با دیگر سیستم‌های موجود مبتنی بر اشتراک دانش مقایسه کرده و سپس برای ارزیابی تاثیر شبکه اجتماعی در بهبود عملکرد سیستم‌های تشخیص نفوذ از شبیه سازی استفاده و عملکرد آن را با دو سیستم پایه Snort و Bro مقایسه کرده‌ایم.

۴-۱ نتایج مقایسه ویژگی‌ها با سیستم‌های مشابه

در جدول (۱) سیستم SNIDS بر اساس چندین ویژگی مختلف که در سیستم‌های تشخیص نفوذ اشتراکی از اهمیت بالاتری برخوردار می‌باشند با دیگر سیستم‌های موجود مبتنی بر اشتراک دانش مقایسه شده است. این مقایسه نشان می‌دهد که در سیستم SNIDS مشکلات موجود در دیگر سیستم‌ها مرتفع گردیده است.

۴-۲ تاثیر شبکه اجتماعی بر عملکرد سیستم تشخیص نفوذ

به منظور ارزیابی سیستم‌های تشخیص نفوذ از روش ارزیابی معرفی شده در [۱۳] استفاده شده که در آن فایل‌های tcpdump در ۷ هفته از داده‌های آموزشی DARPA2000 بکار گرفته می‌شوند. هر فایل به عنوان ورودی به سیستم‌های تشخیص نفوذ(Snort, Bro) داده شده است و این سیستم‌ها به گونه ای پیکربندی شده اند که تمام پیش پردازنده‌ها و قوانین آنها فعال باشد. یک فایل هشدار برای هر فایل tcpdump ایجاد می‌شود. با استفاده از یک برنامه کمکی فایل هشدار با لیست حمله‌ها در فایل tcpdump تطبیق داده می‌شود. تطبیق به معنای انطباق IPها و شماره پورتها یا نوع/کد ICMP می‌باشد و بدین ترتیب هشدارهای مناسب از موارد اشتباه تفکیک می‌گردد. برنامه کمکی همچنین نرخ خطای منفی به ازای هر نوع حمله و نرخ خطای مثبت به ازای هر قانون پایه را گزارش می‌نماید. بعد از اینکه همه حملات و فایل‌های هشدار انطباق داده شدند، برنامه کمکی تعداد خطای مثبت را برای هر قانون و تعداد خطای منفی را به ازای هر نوع حمله شمارش می‌نماید. بعد از آن لیست خطاهای مثبت به منظور حذف موارد تکراری فیلتر می‌گردد. مواردی که قوانین یکسان هشدارهای متعددی را برای یک حمله ایجاد نموده اند. در نهایت یک برنامه کمکی دیگر به منظور محاسبه معیارهای ارزیابی زیر استفاده می‌شود.

True Positive (TP): تعداد نمونه‌های نفوذ که به صورت نفوذ کلاسه بندی شده‌اند.

True Negative (TN): تعداد نمونه‌های نرمال که به صورت نرمال کلاسه بندی شده‌اند.

False Positive (FP): تعداد نمونه‌های نرمال که به صورت نفوذ کلاسه بندی شده‌اند.

False Negative (FN): تعداد نمونه‌های نفوذ که به صورت نرمال دسته بندی شده‌اند.

فرمول ۱: معیارهای ارزیابی سیستم تشخیص نفوذ

$$Detection\ Rate(DTR) = \frac{TP}{TP + FN}$$

$$False\ Positive\ Rate(FPR) = \frac{FP}{TN + FP}$$

$$Overall\ Accuracy(OA) = \frac{TP + TN}{TP + FN + TN + FP}$$

Archvie of SID

جدول ۴: مقایسه مدل پیشنهادی در این مقاله با سیستم‌های تشخیص نفوذ مبتنی بر اشتراک دانش دیگر

معیار / معماری	تنوع در سیستم‌های تشخیص نفوذ	دامنه شبکه تحت پوشش	Single Point Failed	کنترل کننده مرکزی	نحوه تصمیم گیری
مدل اشتراک برای سیستم‌های توزیع شده[۹]	ندارد	سازمانی	دارد	دارد	محلی
یکپارچه سازی سیستم‌ها تشخیص و حفاظت[۱۰]	دارد	سازمانی	دارد	دارد	محلی
شبکه همسایگی مجازی[۱۱]	ندارد	فراسازمانی	ندارد	ندارد	رای گیری
سیستم SNIDS	دارد	اینترنت	ندارد	ندارد	محلی

الف) پارامترهای ارزیابی

در این بخش به منظور بررسی بهبود حاصل از اجرای سیستم SNIDS با استفاده از شبیه‌سازی و در نظر گرفتن پارامتراهای ذیل حالت‌های مختلفی بررسی شده اند. نتایج بدست آمده از این بررسی که به منظور حصول نتایج دقیقتر، میانگین ۱۰ مرتبه تکرار تست می‌باشد، در نمودار شکل (۴) آمده است.

تعداد نودها (سیستم‌های تشخیص نفوذ)، بازه زمانی توزیع، حداکثر پیام قابل مبادله در هر تکرار برای هر نود، نحوه اتصالات شبکه، نوع ارتباط(یکطرفه و دو طرفه)، سیاست توزیع دانش بین همسایه‌ها (ابتدا همسایه‌ها با لینک بیشتر، ابتدا همسایه‌ها با تعداد دوست مشترک کمتر، ترکیب این دو)، تاثیر توپولوژی اتصال(درجه گسستگی گراف) و میزان همپوشانی دانش نودها، پارامترهایی هستند که در ارزیابی این سیستم تاثیرگذار می‌باشند. به منظور ارزیابی اولیه کارایی سیستم مقادیر آمده در جدول (۲) مورد استفاده قرار گرفته اند.

ابتدا سیستم بر اساس مقادیر پارامترها تنظیم شده و یک نود از نوع Snort به عنوان نمونه انتخاب شده است تا تاثیر اشتراک دانش بر عملکرد آن مشخص گردد. سپس بعد از هر ۸ تکرار، وضعیت سیستم ذخیره شده و با استفاده از روش توضیح داده شده ارزیابی صورت می‌گیرد.

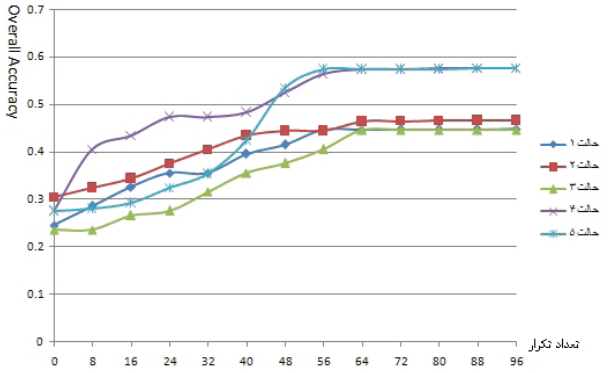
جدول ۵: مقادیر پارامترها در ارزیابی

پارامتر	مقدار
تعداد نودها	۱۵
بازه زمانی توزیع	۵ میلی ثانیه
مجموع دانش موجود در شبکه	۷۲ معادل مجموع قوانین Snort و Bro
حداکثر پیام قابل مبادله	۱ پیام
نحوه اتصالات شبکه	تصادفی
نوع ارتباط	۱۵% یکطرفه و بقیه دو طرفه
سیاست توزیع دانش بین همسایه‌ها	ترکیبی
درجه گسستگی گراف	۱
میزان همپوشانی دانش نودها	۲۰%

ب) نتایج ارزیابی

حالتهای مختلفی که مورد بررسی قرار گرفته اند:

۱- تمام نودها از نوع Snort با بخش‌های مختلف و مجزای پایگاه دانش
۲- تمام نودها از نوع Bro با بخش‌های مختلف و مجزای پایگاه دانش
۳- چندین Snort با بخش‌های مختلف ولی با همپوشانی پایگاه دانش
۴- چندین Snort و Bro با بخش‌های مختلف و مجزا پایگاه دانش
۵- چندین Snort و Bro با بخش‌های مختلف ولی با همپوشانی پایگاه دانش



شکل ۴: نتایج ارزیابی عملکرد IDS در شبکه اجتماعی

همانطور که در شکل (۴) مشاهده می‌شود، با مقایسه تفاوت حالت ۴ و ۵ با سه حالت اول، که در آنها فقط از یک نوع سیستم تشخیص نفوذ استفاده شده است، مشخص می‌شود که با افزایش نوع سیستم تشخیص نفوذ در شبکه، دقت تشخیص سیستم‌ها به میزان ۱۸% افزایش می‌یابد. همچنین با مقایسه حالت‌های ۴و۵ می‌توان نتیجه‌گیری کرد که در صورت وجود همپوشانی بین نودها، در تکرارهای اول دقت تشخیص به کندی رشد می‌نماید که علت آن نیز در تبادل دانش‌های تکراری است.

Archive of SID

۵- نتیجه‌گیری و کارهای آینده

مقایسه انجام شده در جدول (۱) نشان می‌دهد که در معماری پیشنهادی اشکالات موجود (مانند Single Point Failed و کنترل کننده مرکزی) در سیستم‌های دیگر رفع شده است. و همچنین دامنه تحت پوشش و بکارگیری سیستم، گسترش یافته و در عین حال همچنان تصمیم‌گیری، محلی باقی مانده است که از مزایای سیستم SNIDS به شمار می‌آید.

هدف از طراحی سیستم SNIDS، ارایه معماری برای اشتراک دانش بین سیستم‌های تشخیص نفوذ می‌باشد. این سیستم می‌تواند به عنوان مکمل سیستم‌های تشخیص نفوذ فعلی با هر نوع از معماری مورد استفاده قرار گیرد و امکان اشتراک دانش بین سیستم‌هایی از انواع مختلف را فراهم نماید. همانگونه که نتایج نیز نشان می‌دهد، سیستم پیشنهادی با گسترش دامنه تشخیص یک سیستم تشخیص نفوذ، باعث بهبود کارایی آن در شناخت نفوذها می‌گردد. بدیهی است هر چه تنوع دانش‌های به اشتراک گذاشته شده بیشتر باشد نتایج بهتری نیز حاصل خواهد گردید. همچنین برای دستیابی به زمان منطقی در همگرایی بایستی با افزایش تعداد نودها، تعداد دانش قابل مبادله افزایش و یا زمان توزیع کاهش یابد.

در ادامه این تحقیق می‌توان فعالیت‌های پژوهشی بسیاری از جمله آنچه در ادامه آمده است بر روی این سیستم انجام داد:

- تحلیل تاثیر پارامترهای مختلف در عملکرد سیستم و استخراج حالت بهینه
- استفاده از سیستم‌های تشخیص نفوذ ناهمگون و مبتنی بر رفتار در شبکه
- پالایش دانش‌های نفوذ بر اساس تجارب اشتراکی
- جلوگیری از انتشار دانش‌های اشتباه در شبکه اجتماعی
- حفاظت از سیستم‌های عضو در شبکه در مقابل نفوذگران احتمالی به شبکه

مراجع

[1] Martin Roesch and further work from Chris Green. “Snort Rules”, http://www.snort.org/

[2] http://www.bro-ids.org/

[3] Lippmann, R. P., D. J. Fried, I. Graf, J. W. Haines, K. Kendall, D. McClung,D. Weber, S. Webster, D. Wyschogrod, R. K. Cunningham, and M. Zissman, Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation. In Proc. of the DARPA Information Survivability Conference and Exposition, Los Alamitos, CA. IEEE Computer Society Press

[4] Phillip A. Porras, Peter G. Neumann, “*EMERALD: event monitoring enabling responses to anomalous live disturbances*”, In 1997 National Information Systems Security Conference, October 1997

[5] S. Snapp, J. Brentano, G. Dias et al., “*DIDS (Distributed Intrusion Detection System) – motivation, architecture, and an early prototype”,* Proceedings of the 14th National Computer Security Conference, October 1991

[6] S. Staniford-Chen, S. Cheung, R. Crawford, M. Dilger, J.Frank, J. Hoagland, K. Levitt, C. Wee, R. Yip, and D. Zerkle, “*GrIDS-a graph based intrusion detection system for large networks*”, Proceedings of the 19th National Information Systems Security Conference, September 1996

[7] Jai Sundar Balasubramaniyan, Jose Omar Garcia-Fernandez, David Isacoff, Eugene Spafford, and Diego Zamboni. “*An architecture for intrusion detection using autonomous agents*”, Proceedings of the Fourteenth Annua Computer Security Applications Conference, pp 13–24, IEEE Computer Society, December 1998

[8]] Eugene H. Spafford and Diego Zamboni. “*Intrusion detection using autonomous agents*”, Computer Networks, 34 (4):547–570, October 2000

[9] Tao Peng, Christopher Leckie, “Information sharing for distributed intrusion detection systems”, 2007

[10] Karen Scarfone, Peter Mell, “Guide to Intrusion Detection and Prevention Systems”, 2007

[11] Geetha Ramachandran, Delbert Hart, “A P2P intrusion detection system based on mobile agents”, 2004

[12] Cisco Systems, “Wireless LAN Controller IDS Signature Parameters”, http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a008063e5d0.shtml, 2007

[13] S Terry Brugger, Jedadiah Chow, “An Assessment of the DARPA IDS Evaluation Dataset Using Snort” , 2005.