به نام خداوند جان و خرد

کزین برتر اندیشه برنگذرد

دانشگاه صنعتی امیرکبیر (پلی تکنیک تهران)

دانشکده کامپیوتر و فناوری اطلاعات

پایان نامه کارشناسی ارشد

در رشته فناوری اطلاعات گرایش امنیت اطلاعات

یک رویکرد مانا با استفاده از رای‌گیری برای سیستم تشخیص نفوذ توزیع شده

نگارش

علی زند

استاد راهنما

دکتر بابک صادقیان

۱۳۸۵

بسمـه تعالـــی

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)
معاونت پژوهشی

فرم اطلاعات پایان نامه
کارشناسی ارشد و دکترا

تاریخ: .....

پیوست: .....

نام و نام خانوادگی:	علی زند	**دانشجوی آزاد** ■	**بورسیه** □	**معادل** □
شماره دانشجوئی:	۸۳۱۳۱۱۱۱	**دانشکده:** مهندسی کامپیوتر	**رشته تحصیلی:**	امنیت اطلاعات
نام و نام خانوادگی استاد راهنما:	بابک صادقیان			
عنوان پایان نامه به فارسی:	یک رویکرد مانا با استفاده از رای‌گیری برای سیستم تشخیص نفوذ توزیع شده			
عنوان پایان نامه به انگلیسی:	A Survivable Approach, with a Voting Scheme for Distributed Intrusion Detection			
نوع پروژه:	**کارشناسی ارشد** ■ / **دکترا** □	**کاربردی** □	**بنیادی** □	**توسعه ای** ■ **نظری** □
تاریخ شروع:		**تاریخ خاتمه:**	**تعداد واحد:**	۶
سازمان تأمین کننده اعتبار:				
واژه های کلیدی به فارسی:	سیستم تشخیص نفوذ توزیع‌شده، معماری سلسله‌مراتبی، تحمل‌پذیری حمله، رای‌گیری			
واژه های کلیدی به انگلیسی:	Distributed Intrusion Detection, Hierarchical Architecture, Attack Tolerance, Voting			

نظرها و پیشنهادها به منظور بهبود فعالیت های پژوهشی دانشگاه:

استاد راهنما:

دانشجو:

امضاء استاد راهنما: **تاریخ:**

نسخه ۱: معاونت پژوهشی
نسخه ۲: کتابخانه و به انضمام دو جلد پایان نامه به منظور تسویه حساب با کتابخانه و مرکز اسناد و مدارک علمی

تقدیم به

پدر و مادر عزیزم

با تشکر فراوان از استاد ارجمندم، جناب آقای دکتر بابک صادقیان کـه مـرا در تمـام طـول اجـرای پروژه با راهنمایی‌های دقیق، موشکافانه و دلسوزانه یاری نمودند.

چکیده

با گسترش روزافزون شبکه‌های کامپیوتری و اینترنت و با افـزایش پیچیـدگی حمـلات کـامپیوتری، عمل تشخیص نفوذ روزبروز مشکل‌تر شده و حتی خود سیستم‌های تشخیص نفوذ نیـز تبـدیل بـه هدف حملات شده‌اند. یکی از معماری‌های توزیع‌شده تشخیص نفوذ که در عمل موفق‌تـر از سـایر معماری‌های توزیع‌شده بوده است، معماری سلسله‌مراتبی است کـه یکـی از مشـکلات اصـلی ایـن معماری، وجود نقاط حساس متعدد در آن است. در این پایان‌نامه روشی بـرای از بـین بـردن نقـاط حساس معماری سلسله‌مراتبی، با استفاده از رای‌گیری ارائه شده است. در روش پیشنهادی، بـا ایـن فرض که نودها هم‌شأن هستند، هیچ‌یک نسبت به دیگری ارجحیت ذاتی ندارند. در ادامه، معمـاری پیشنهادی تحلیل شده و حداقل تعداد نودهای تسخیر شده لازم جهت تسخیر ریشه محاسبه گشـته است و در نهایت، یک نمونه از این معماری، پیاده‌سازی شده و کارایی آن مورد آزمون قـرار گرفتـه است. سیستم پیاده‌سازی‌شده توانایی اداره کردن یک حمله در هر ۸۰ ثانیه را دارد.

کلمات کلیدی: سیستم تشخیص نفوذ توزیع‌شده، معمـاری سلسـله‌مراتبـی، تحمـل‌پـذیری حملـه، رای‌گیری

فهرست مطالب

۱ ـ مقدمه

امروزه در دنیای کامپیوترها و عصر ارتباطات زندگی می‌کنیم و کامپیوترها در امور روزمره مردم دخالت دارند. در چنین دنیایی، امنیت کامپیوترها و شبکه های کامپیوتری اهمیت فوق‌العاده‌ای پیدا می‌کند. اقداماتی که در سیستم‌های کامپیوتری بمنظور تامین امنیت استفاده می‌گردد به دو گروه زیر تقسیم می‌گردد[1]:

- اقدام محافظتی[1]: یعنی سیستم بگونه‌ای طراحی و ساخته شود که جلوی حمله گرفته شود.
- اقدام مقابله‌ای[2]: یعنی در صورت حمله به سیستم، اقدام متقابلی در برابر شخص مهاجم انجام شود و بدین ترتیب، شخص مهاجم بخاطر ترس از اقدام متقابل، از تهاجم صرف نظر کند.

همانطور که مشخص است و در ضرب‌المثلی فارسی نیز آمده است: "پیش‌گیری بهتر از درمان است". معادل این جمله را در حفظ امنیت سیستمها می‌توان بدین صورت درآورد که: "امن نگه داشتن بهتر از اقدام متقابل است". اما مشکل از اینجا ناشی می‌شود که امن نگه داشتن سیستمها (مانند پیش‌گیری) همیشه ممکن، و یا حداقل مقرون بصرفه نیست. بهمین دلیل معمولا از ترکیبی از دو روش فوق استفاده می‌شود، بدین صورت که در وهله اول سعی می‌شود سیستم بصورت امن طراحی شود، ولی در کنار آن، مکانیزم‌هایی برای اقدام متقابل در سیستم در نظر گرفته می‌شود. برای انجام اقدام متقابل، در ابتدا نیاز است که عمل خصمانه مهاجم شناسایی شود. سیستمهایی که برای این منظور مورد استفاده قرار می‌گیرند، سیستم تشخیص نفوذ[3] نام دارند.

تشخیص نفوذ، عبارتست از مساله شناسایی استفاده غیر مجاز و سوء استفاده از سیستم کامپیوتری، توسط نفوذگران داخلی یا خارجی، یا بعبارت دیگر شناسایی کسانی که بدون اجازه از سیستم کامپیوتری استفاده می‌کنند و یا اجازه استفاده از کامپیوتر را دارند ولی از حقوق خود تجاوز می‌کنند. سیستم‌های تشخیص نفوذ بر اساس این ایده کار می‌کنند که رفتار نفوذگر بطور قابل توجهی با رفتار کاربر عادی متفاوت است.

---

[1] safeguard
[2] countermeasure
[3] Intrusion Detection System (IDS)

با افزایش آگاهی و تکنیک‌هایی که مهاجمین در حمله به شبکه‌ها بکار می‌برند و همچنین افزایش روزبروز ابزارهای حمله‌ای که در اختیار مهاجمین قرار دارد، روز بروز بر پیچیدگی عمل تشخیص نفوذ افزوده می‌شود و حتی خود این سیستم‌ها تبدیل به هدف مناسبی برای مهاجمین شده‌اند بطوریکه ابزارهایی برای فریب سیستم‌های تشخیص نفوذ[1] و یا حمله به آنها طراحی شده‌اند. مهاجمین می‌دانند که با از کار انداختن سیستم‌تشخیص نفوذ می‌توانند ردپای اعمال خود را مخفی نگاه دارند و از اقدام متقابل مصون بمانند. با توجه به پیچیده‌تر شدن وظایف سیستم‌های تشخیص نفوذ، امن نگاه داشتن آنها مشکل‌تر می‌شود، زیرا پیچیدگی همواره باعث عدم توانایی طراح سیستم در تحلیل امنیتی سیستم می‌گردد. روزبروز بر تعداد آسیب‌پذیری‌هایی که در سیستم‌های تشخیص نفوذ یافته می‌شوند افزوده می‌شود. علت این امر این است که با افزایش پیچیدگی حملات، زبان‌هایی که برای توصیف حملات و شناساندن آنها به IDS مورد استفاده قرار می‌گیرند، کارایی خود را از دست داده و نیاز به توسعه پیدا می‌کنند تا توان بیان آنها افزایش یابد. این افزایش توان به پیچیدگی کد موتور تحلیل IDS منجر می‌شود که به نوبه خود باعث ناامن‌تر شدن آن می‌گردد.

امروزه با گسترش روزبروز سیستم‌های تشخیص نفوذ توزیع‌شده لایه دیگری از پیچیدگی به این سیستم‌ها اضافه شده است.

۱-۲- دسته‌بندی سیستم‌های تشخیص نفوذ

سیستم‌های تشخیص نفوذ را می‌توان بر اساس معیارهای مختلفی به دسته‌های متفاوتی تقسیم کرد.

۱-۲-۱ دسته‌بندی بر اساس منبع داده

- سیستم‌های تشخیص نفوذ، بر اساس منبع داده مورد استفاده به سه دسته تقسیم می‌شوند:
- سیستم‌های مبتنی بر میزبان: این سیستم‌ها از مجموعه اطلاعات میزبان برای تشخیص نفوذ استفاده می‌کنند.

[1] IDS evasion tools

- سیستم‌های مبتنی بر شبکه: این سیستم‌ها از اطلاعات و بسته‌های شبکه، برای تشخیص نفوذ استفاده می‌کنند.
- سیستم‌های ترکیبی[1]: این سیستم‌ها هم از اطلاعات میزبان‌ها و هم از اطلاعات بسته‌های شبکه استفاده می‌کنند.

۲.۱.۱ دسته‌بندی بر اساس معماری

سیستم‌های تشخیص نفوذ را از لحاظ معماری می‌توان به دو دسته توزیع شده و منفرد[2] تقسیم‌بندی کرد. سیستم‌های تشخیص نفوذ توزیع شده، دارای استعداد بیشتری نسبت به سیستم‌های تشخیص نفوذ منفرد در تشخیص حملات متنوع هستند و به طور کلی، نسبت به سیستم‌های تشخیص نفوذ منفرد دارای سه مزیت زیر هستند:

- برخی حملات، با استفاده از سیستم‌های تشخیص نفوذ منفرد قابل شناسایی و یا حداقل قابل شناسایی دقیق نیستند.
- استفاده از سیستم‌های تشخیص نفوذ توزیع‌شده، با توجه به منابع اطلاعاتی وسیع‌تری که این سیستم‌ها در اختیار دارند، مقدار خطای مثبت، یا به عبارتی اخطارهای اشتباه را کاهش می‌دهد.
- امکان مدیریت امنیتی کل شبکه بصورت متمرکز توسط سیستم‌های تشخیص نفوذ توزیع‌شده فراهم می‌آید.

عیبهای اصلی این سیستم‌ها عبارتند از:

- پیچیدگی پیاده‌سازی: پیاده‌سازی یک سیستم توزیع‌شده، همواره پیچیده‌تر از پیاده‌سازی منفرد همان سیستم است.

---

[1] hybrid
[2] standalone

- پیچیدگی امنیت: امنیت یک سیستم توزیع‌شده دارای فاکتورهایی اضافه بر فاکتورهای امنیتی سیستم‌های منفرد است.

۲ ۱ -سیستم‌های تشخیص نفوذ توزیع‌شده

سیستم‌های تشخیص نفوذ توزیع‌شده سیستم‌های تشخیص نفوذی هستند که دارای جمع‌آوری داده توزیع‌شده، تصمیم‌گیری توزیع‌شده، پاسخ توزیع‌شده و یا ترکیبی از این موارد هستند. صفت توزیع‌شدگی در اینجا به خود سیستم باز می‌گردد و نه به نفوذ. به عبارت دیگر سیستم‌های تشخیص نفوذ توزیع‌شده لزوما قادر به تشخیص حملات توزیع‌شده نمی‌باشند.

مطابق با [2] سیستم‌های تشخیص نفوذ توزیع شده دارای معماری‌های زیر هستند:

- معماری سلسله مراتبی
- معماری شبکه‌ای
- معماری ترکیبی
- معماری عامل‌های متحرک

در معماری سلسله‌مراتبی، نودهای تشخیص نفوذ، در یک درخت سلسله‌مراتب[1] قرار می‌گیرند بطوریکه هر نود، غیر از نود ریشه دارای یک نود پدر است و همچنین هر نود غیر از نودهای برگ دارای یک یا چند فرزند است. درخت سلسله‌مراتب این معماری، مشابه سلسله‌مراتب مدیریتی در سازمان‌های انسانی است، بدین معنا که اطلاعات در درخت از پایین به بالا و دستورها از بالا به پایین حرکت می‌کنند.

در معماری شبکه‌ای، نودهای تشخیص نفوذ دارای ساختار مشخصی نیستند و هریک از نودها می‌تواند با هر نود دلخواه دیگری ارتباط برقرار کند. در این معماری ارتباطات بصورت همتا به

[1] hierarchy tree

همتا[1] است، یعنی هیچ نودی دارای مزیتی بر دیگری نیست و نودها تنها با یکدیگر همکاری می‌کنند.

در معماری ترکیبی، سعی شده است مزایای معماری‌های سلسله‌مراتبی و شبکه‌ای با یکدیگر ترکیب شوند. در این معماری، نودهای تشخیص نفوذ در یک درخت سلسله‌مراتب پیش‌فرض قرار می‌گیرند ولی بر خلاف معماری سلسله‌مراتبی می‌توانند توسط بعضی مسیرهای رزرو شده خارج از درخت، با یکدیگر ارتباط برقرار کنند.

معماری عامل‌های متحرک را نمی‌توان یک معماری خاص بحساب آورد، بلکه بایستی آنرا فناوری‌ای دانست که ترکیب آن با معماری‌های موجود، معماری‌های قدرتمند و متفاوتی را می‌سازد. مزیت اصلی معماری‌های مبتنی بر عامل این است که در این معماری‌ها بجای انتقال اطلاعات بین میزبان‌های مختلف، برای عمل تشخیص نفوذ، عامل‌های متحرک بین میزبان‌ها جابجا می‌شوند.

معماری سلسله‌مراتبی نسبت به معماری شبکه‌ای دارای قابلیت مقیاس‌پذیری است که علت این قابلیت، وجود ارتباطات کارا در این معماری است. اگر دو نود مفروض را در درخت سلسله‌مراتب در نظر بگیریم، تنها یک راه ارتباطی برای ارتباط این دو عنصر وجود دارد که این مسیر، از نزدیکترین پدر مشترک آنها می‌گذرد. اکثر معماری‌های سیستم‌های تشخیص نفوذ توزیع‌شده‌ای که امروزه مورد استفاده قرار می‌گیرند، معماری سلسله‌مراتبی هستند، ولی معماری‌های سلسله‌مراتبی با وجود این مزایا، دارای معایبی نیز هستند. یکی از مشکلات مهم این معماری، وجود نقاط حساس متعدد در این درخت سلسله‌مراتب است. بعبارت دیگر بعلت وجود مسیرهای ثابت اطلاعاتی، در صورت بروز اشکال در نودهای بالایی درخت سلسله‌مراتب به طوری که نتوانند وظیفه خود را بدرستی انجام دهند، درصد زیادی از مسیرهای اطلاعاتی مختل شده و سیستم، تمام و یا قسمت عمده‌ای از توانایی خود در تشخیص توزیع‌شده نفوذ را از دست می‌دهد. برای رفع این مشکل در سیستم‌های تشخیص نفوذ سلسله‌مراتبی، تلاش‌های زیادی صورت گرفته است که می‌توان از روی

[1] peer to peer

آوردن به معماری‌های شبکه‌ای و عامل متحرک به عنوان نمونه‌هایی نام برد، ولی هیچ‌یک از این روش‌ها نتوانسته‌اند به موفقیت سیستم‌های تشخیص نفوذ سلسله‌مراتبی عمل نمایند. یکی از مشکلات عمده روش‌های رقیب، وجود مسیرهای متعدد اطلاعاتی در این سیستم‌ها است که نسبت به افزایش اجزای سیستم تشخیص نفوذ، با مرتبه دو زیاد می‌شوند و مدیریت این مسیرها را بسیار دشوار و یافتن یک اطلاعات خاص در سیستم را مشکل‌تر می‌کنند. این مشکل در نهایت منجر به عدم مقیاس‌پذیری این معماری‌ها می‌شود. از طرفی وجود ارتباطات کارا منجر به مشکل عدم تحمل‌پذیری معماری سلسله‌مراتبی حاصل در برابر حملات می‌گردد. علت این امر این است که نودهای بالایی در درخت سلسله‌مراتب می‌توانند هدف‌های خوبی برای مهاجمان باشند. زیرا یک مهاجم می‌تواند با از کار انداختن نودهای بالایی، بخش بزرگی از کارایی سیستم تشخیص نفوذ را مختل نماید. بنابراین با ارائه روشی برای تحمل‌پذیر نمودن معماری سلسله‌مراتبی در برابر حملات، یکی از موانع مهم استفاده از این معماری کارا در سیستم‌های تشخیص نفوذ برطرف می‌گردد.

یکی از زمینه‌های فعال تحقیقاتی امنیت، زمینه تحمل‌پذیری حملات است که هدف این زمینه، تحمل‌پذیرسازی سرویس‌ها و بخصوص سرویس‌های توزیع شده در برابر حملات می‌باشد. زمینه تحمل‌پذیری حملات، با زمینه تحمل‌پذیری خطا ارتباط بسیار نزدیکی دارد. سه روش اصلی برای تحمل‌پذیری سیستم تشخیص نفوذ در برابر حملات وجود دارد:

- تقویت کنترل دسترسی
- جلوگیری از کشف و شناسایی[1]
- افزونگی[2]

[1] detection and identification obstructing

[2] redundancy

– در روش تقویت کنترل دسترسی سعی می‌شود در وهله اول سیستم در برابر حمله مهاجم، تحمل‌پذیر شود یا بعبارت دیگر، با طراحی مدل‌ها و مکانیزم‌های کنترل دسترسی جدید و قوی‌تر، سعی می‌شود حمله به سیستم غیر ممکن ویا بسیار مشکل شود.

– در روش جلوگیری از کشف و شناسایی، سعی می‌شود سیستم مورد نظر (که در اینجا سیستم تشخیص نفوذ توزیع‌شده است) از دید مهاجم پنهان بماند. واضح است که حمله به سیستمی که مکان و خصوصیات آن مشخص نیست، بسیار سخت‌تر از سیستمی است که این اطلاعات در مورد آن موجود است.

– در روش افزونگی سعی می‌شود مکانیزم‌های رزرو و افزونه‌ای در داخل سیستم مورد نظر تعبیه شود تا اگر یکی یا تعداد محدودی از اجزای سیستم توسط مهاجم، دچار مشکل گشتند، سیستم بتواند در نبود آنها به اجرای وظایف خود ادامه دهد.

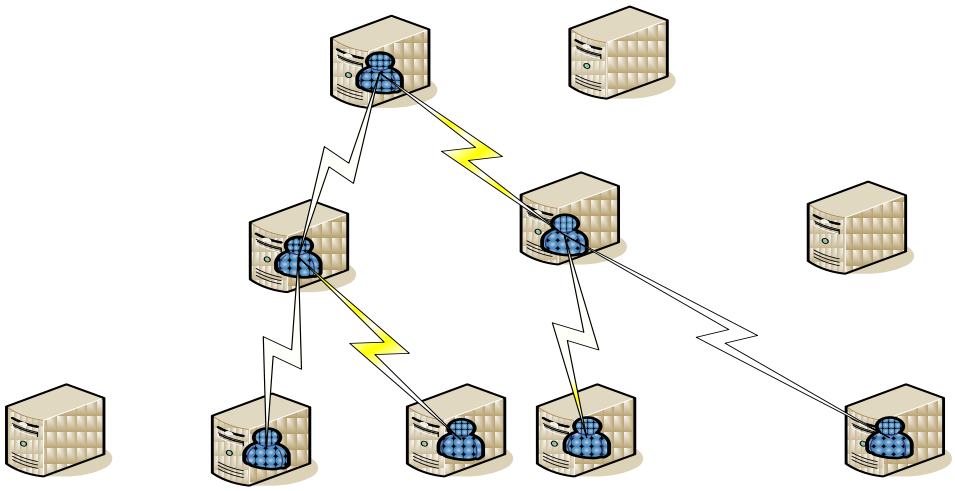
اگر امکان پیاده‌سازی یکی از این روش‌ها بدون نقص و با کارایی صد در صد وجود داشت، آنگاه وجود سایر روش‌ها لزومی نداشت، ولی مشکل از آنجایی ناشی می‌شود که تضمین صد در صد درست کار کردن، برای هیچ‌یک از این روش‌ها وجود ندارد. به همین خاطر سعی می‌شود از ترکیبی از سه روش فوق برای مستحکم کردن سیستم‌ها در برابر حملات استفاده شود. به استراتژی به کارگیری لایه‌های متفاوتی از امنیت، دفاع در عمق[1] گفته می‌شود که یکی از روش‌های شناخته شده در امن کردن سیستم‌ها است.

روش تقویت کنترل دسترسی از محدوده مطالب این پایان‌نامه خارج است. مدل‌های کنترل دسترسی زیادی تا کنون ارائه شده‌اند و روز به روز بر تعداد آن‌ها افزوده می‌شود.

اشخاصی مانند Mell در [3] سعی کردند با ترکیب روش سلسله‌مراتبی با سایر روش‌ها، ضمن استفاده از مزایای معماری سلسله‌مراتبی، مشکل وجود نقاط حساس متعدد را در این معماری حل نمایند. در معماری پیشنهاد شده توسط Mell، نودهای تشخیص نفوذ در یک درخت سلسله‌مراتبی

[1] defence in depth

قرار می‌گیرند. تفاوت این معماری با معماری‌های سلسله‌مراتبی قدیمی‌تر در این است که در معماری Mell، نودهای تشخیص نفوذ غیر برگ، عامل‌های متحرک هستند. با استفاده از ویژگی تحرک، در زمان احساس خطر، عامل‌ها جابجا می‌شوند و پیدا کردن نودهای بالایی درخت سلسله‌مراتب را برای مهاجم دشوار می‌نمایند.



شکل ۱-۱ - ارتباط اجزا در معماری Mell

در شکل ۱-۱ یک درخت سلسله‌مراتب نمونه در معماری Mell نمایش داده شده است. در این شکل هر میزبان نماینده نودهایی در شبکه است که از عامل متحرک پشتیبانی می‌کنند و بنابراین عامل‌ها می‌توانند به آنها منتقل شده و بر روی آنها اجرا گردند. هر آدمک نشان‌دهنده یک عامل است که بر روی یک میزبان در حال اجرا است و اتصالات بین عامل‌ها رابطه پدر–فرزندی را نشان می‌دهد.

در این معماری نیاز به وجود تعداد زیادی از میزبان‌ها که از عامل‌های متحرک پشتیبانی می‌کنند است که تعداد کل این میزبان‌ها بایستی بیشتر از تعداد کل نودهای تشخیص نفوذ موجود در درخت سلسله‌مراتب باشد. این معماری تکیه بر توانایی هر نود در تشخیص خطر و توانایی او در