بسم الله الرحمن الرحيم

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان‌نامه‌ی دکتری رشته‌ی مهندسی کامپیوتر گرایش نرم‌افزار

همبسته‌سازی هشدارها به‌کمک سیستم ایمنی مصنوعی

استاد راهنما:

دکتر احمد براآنی دستجردی

استاد مشاور:

دکتر عباس رضائی

پژوهشگر:

مهدی باطنی

مهر ماه۱۳۹۱

دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه‌ی دکتری رشته‌ی مهندسی کامپیوتر گرایش نرم‌افزار آقای مهدی باطنی تحت عنوان

همبسته‌سازی هشدارها به کمک سیستم ایمنی مصنوعی

در تاریخ ۹۱/۷/۱۱ توسط هیأت داوران زیر بررسی و با درجه عالی به تصویب نهایی رسید.

۱- استاد/ استادان راهنمای پایان‌نامه دکتر ...احمد براآنی... با مرتبه‌ی علمی ...دانشیار... امضا

۲- استاد/ استادان مشاور پایان‌نامه دکتر ...عباس رضائی... با مرتبه‌ی علمی ...استاد... امضا

۳- استاد/ استادان داور داخل گروه دکتر ...کامران زمانی‌فر... با مرتبه‌ی علمی ...دانشیار... امضا

۴- استاد/ استادان داور داخل گروه دکتر ...بهروز ترک لادانی... با مرتبه‌ی علمی ...دانشیار... امضا

۵- استاد/ استادان داور خارج از گروه دکتر ...محسن کاهانی... با مرتبه‌ی علمی ...دانشیار... امضا

امضای مدیر گروه

سپاسگذاری:

در اینجا بر خود لازم می‌دانم مراتب سپاس خود را به پیشگاه کلیه‌ی اساتیدی که در طی این دوره‌ی پژوهشی از دانش آنها بهره گرفته‌ام تقدیم دارم. بویژه استاد محترم راهنمایم جناب آقای دکتر احمد براآنی که همواره با صبر، متانت و دقت در راهگشایی مشکلات بوجود آمده مرا یاری نمودند و اگر راهنمایی‌های ارزشمند ایشان نبود به سرانجام رساندن این پژوهش میسر نمی‌شد. همچنین از جناب آقای دکتر عباس رضائی که مشاوره‌ی این پایان‌نامه را بعهده داشته‌اند صمیمانه سپاسگذاری می‌کنم. همچنین از جناب آقای دکتر علی قربانی ریاست محترم دانشکده علوم کامپیوتر دانشگاه نیوبرونسویک کانادا که در طی دوران فرصت مطالعاتی از دانش و تجربیاتشان به وفور بهره بردم صمیمانه سپاسگذاری می‌نمایم.

این پایان‌نامه پیشکشی است ناچیز به‌رسم قدردانی به تمامی آنها که برایم عزیزند، پدر و مادر بزرگوارم که با تمام توان از ابتدایی‌ترین دوران دانش‌اندوزی تا امروز همیشه مشوق و پشتیبان من بوده‌اند، همسر مهربانم که در تمام دوران پر فراز و نشیب تحصیلات دکتری در تمامی سختی‌ها یار و یاور من بوده‌است و دستیابی به این هدف سترگ بدون پشتیبانی‌های او میسر نمی-شد و تمامی اساتید و آموزگارانی که در مقاطع مختلف تحصیلی از دانش و فضائل اخلاقی آنها بهره برده‌ام.

چکیده:

سیستم تشخیص نفوذ (IDS) وظیفه‌ی نظارت بر رویدادهایی که در یک کامپیوتر و یا شبکه‌ی کامپیوتری رخ می‌دهد و تحلیل این رویدادها برای یافتن نشانه‌های نفوذ را بعهده دارد. منظور از نفوذ، تلاشی از طرف یک کاربر مجاز یا غیر مجاز است که نتیجه‌ی موفقیت آن به خطر افتادن محرمانگی، یکپارچگی، در دسترس بودن و یا عبور از مکانیزمهای امنیتی می‌باشد. معمولا IDS در صورت تشخیص یک نفوذ با تولید یک هشدار مدیر امنیتی سیستم را از خطر بوجودآمده آگاه می‌کند. اما در یک شبکه‌ی کامپیوتری گسترده با دهها و یا صدها کاربر، تعداد هشدارهای تولید شده آنقدر زیاد خواهد شد که مدیر امنیتی سیستم قادر به تحلیل هشدارها و استفاده از آنها نخواهدبود. شناخته‌شده‌ترین راه‌حل برای مواجه با مشکلِ تعدادِ زیادِ هشدارها، همبسته-کردن آنهااست. همبسته‌سازی هشدارها روند تحلیل هشدارهای تولیدشده توسط یک یا بیش از یک IDS و ایجاد یک دید کلی و سطح بالا نسبت به مخاطرات و یا حملاتِ در شرف وقوع می‌باشد. سیستم همبسته‌ساز معمولا این کار را با حذف هشدارهای کاذب، گروه‌بندی هشدارهایی که به یک رویداد مربوط می‌شوند و اولویت‌بندی هشدارها انجام می‌دهد. روشهای مختلفی برای انجام همبسته‌سازی هشدارها استفاده شده‌اند که آنها را به سه دسته‌ی کلیِ مبتنی بر همجوشی هشدارها، مبتنی بر فیلترکردن هشدارها و مبتنی بر کشف روابط سببی بین هشدارها تقسیم کرده‌اند. هیچ یک از روشهای مطرح شده به تنهایی قادر به تامین همه‌ی اهداف همبسته‌سازی نیستند. ضمن آنکه هریک دارای کاستی‌های خاص خود نیز می‌باشند. روش‌های ترکیبی از ترکیبی از روشهای سه‌گانه‌ی فوق برای دستیابی به بهترین نتیجه استفاده می‌کنند. اما چالش اصلی برای روشهای ترکیبی یافتن ساختار ترکیبی مناسبی است که علاوه بر داشتن نقاط قوت هر یک از روش‌ها از کاستی‌های آنها نیز به دور باشند. رویکردهای مختلفی برای ارائه‌ی معماری‌ها ترکیبی وجود داشته‌است. در این پایان‌نامه یک معماریِ ترکیبیِ سه لایه به‌نام iCorrelator پیشنهاد شده‌است. هدف iCorrelator آن است که همبسته‌سازی هشدارها با کمترین نیاز به دانش اولیه و بصورت پویا انجام شود در عین حال و بصورت همزمان کارایی و دقت همبسته‌سازی نیز بهبود یابد. معماریِ سه‌لایه‌ی iCorrelator با الهام گرفتن از ساختار سیستم ایمنی بدن انسان طراحی شده‌است که مبتنی بر پاسخهای سیستم ایمنی مادرزادی، پاسخهای اولیه‌ی سیستم ایمنی اکتسابی و پاسخهای ثانویه‌ی سیستم ایمنی اکتسابی می‌باشد. علاوه بر این از لحاظ عملکردی نیز iCorrelator از یکی از الگوریتمهای شناخته‌شده‌ی سیستم ایمنی مصنوعی به‌نام AIRS برای یادگیری با نظارت استفاده می‌کند. معماری سه-لایه‌ی iCorrelator از ترکیبی از دانش اولیه‌ی محدود در قالب قوانین عمومیِ غیر وابسته به حملاتِ خاص برای مواجه با حالات پیش‌بینی شده، یک الگوریتم یادگیریِ بانظارت برای مواجه با حالات جدید و پیش‌بینی نشده و همچنین سلولهای حافظه‌ی ایمنی برای بخاطر سپردن این حالات جدید برای مواجه‌های بعدی استفاده می‌کند. هدف از بکارگیری این ساختار ترکیبی سه‌لایه در iCorrelator برخورداری از دقت در عین کارایی و پویایی می‌باشد. مجموعه‌های داده‌ای DRPA2000 وhoneynet netForensics برای بررسی دقت و کارایی iCorrelator مورداستفاده قرارگرفته‌اند. سه معیار کمال، درستی و نرخ‌خطا در همبسته‌سازی برای بررسی دقت و همچنین زمان اجرا برای بررسی کارایی iCorrelator مورد استفاده - قرارگرفته‌است. برای کلیه‌ی داده‌های مورد استفاده، iCorrelator توانسته است به صورت پویا و بدون داشتن دانش اولیه‌ای از حملات موجود در مجموعه‌های داده‌ای، حملات را استخراج و گراف حمله را نمایش دهد. iCorrelator از لحاظ دقت قابل مقایسه با روشهایی است که با استفاده از تعداد بسیار زیادی از قوانینِ ویژه همین حملات را تشخیص می‌دهند (پویا نیستند) و از لحاظ کارایی نیز از روشهای پویای موجود بهتر عمل می‌کند بطوری که زمان آموزش آن بسیار کوتاه است و فرآیند یادگیری با جمع‌آوری اطلاعات به صورت پویا و در حین پردازش هشدارها انجام می‌شود. توانایی iCorrelator در استخراج حملاتی که هیچ گونه اطلاع قبلی از کیفیت وقوع آنها ندارد و ارائه‌ی گراف حمله‌ی آنها، شاهدی بر صحت عملکرد پویای آن می‌باشد.

واژگان کلیدی:

همبسته‌سازی هشدارها، سیستم تشخیص نفوذ، سیستم ایمنی مصنوعی، الگوریتم سیستم تشخیص ایمنی مصنوعی

فهرست مطالب

عنوان **صفحه**

عنوان **صفحه**

عنوان **صفحه**

عنوان **صفحه**

عنوان **صفحه**

فهرست شکلها

عنوان **صفحه**

عنوان **صفحه**

عنوان **صفحه**

فهرست جدول‌ها

عنوان **صفحه**

فصل اول

معرفی

با توجه به‌گسترش استفاده از شبکه‌های کامپیوتری و کاربرد فراگیر آن در مدیریت جنبه‌های مختلف زندگیِ امروزی، اهمیتِ تامین امنیت اطلاعاتِ نگهداری شده و مبادله شده روزبه‌روز بیشتر آشکار می‌شود. به‌گونه‌ای که امنیت اطلاعات در مبادلات الکترونیکی یکی از مهمترین دغدغه‌های فکریِ کاربران برای استفاده یا عدم استفاده از سیستم‌های کامپیوتری‌است. امنیت اطلاعات دارای جنبه‌های مختلفی است بر همین اساس ابزارها و روش‌های مختلفی برای تامین جنبه‌های مختلف امنیت پیش‌بینی شده‌است. روش‌های رمزنگاری، پروتکل‌های امنیتی، کنترل دسترسی، آنتی‌ویروس‌ها، دیوارهای آتش و سیستم‌های تشخیص نفوذ[1] هریک در سطحی با تامین امنیت اطلاعات سروکار دارند. با توجه به اینکه امکانِ تعریف همه‌ی اعمال غیرمجاز در یک سیستم و یا شبکه‌ی کامپیوتری وجود ندارد و از طرفی اعمالی وجود دارند که بخودی‌خود مجاز هستند اما ازترکیب آن‌ها می‌توان یک هدف غیرمجاز را عملی‌کرد لذا دامنه‌ی اِعمالِ محدودیت بر توانایی‌های کاربران، معمولا دارای محدودیت می‌شود. در این بین سیستم-های تشخیص نفوذ (IDS) به‌بررسیِ رفتارهای کاربرانِ یک سیستم یا یک شبکه‌ی کامپیوتری می‌پردازند تا سوءاستفاده‌های احتمالی کاربران را از اعمالی که مجاز به انجام آن هستند شناسایی و گزارش نمایند. به‌این‌ترتیب IDS به یکی از اجزاء اساسی امنیتی در سیستم‌های کامپیوتری تبدیل شده‌است و روزبه‌روز نیز بر اهمیت و میزان استفاده از آن افزوده می‌شود.

---

[1] Intrusion Detection System (IDS)

معمولا یک IDS با مشاهده‌ی یک عمل مشکوک ضمن تولید هشدار برای آن عمل، مدیر امنیتی سیستم را از انجام آن آگاه می‌کند. با توجه به گسترش شبکه‌های کامپیوتری و ایجاد شبکه‌های گسترده با صدها و یا هزاران سیستم، تعداد هشدارهای امنیتی تولیدشده توسط IDS یا IDSهای موجود در شبکه بسیار زیاد می‌شود. به علت زیادیِ هشدارها و کم‌اهمیت‌بودن نسبی هر یک از آن‌ها، شناسایی مخاطرات امنیتی و تصمیم‌گیریِ درست در مورد آن‌ها برای مدیر سیستم بسیار مشکل خواهدبود. علاوه بر این اغلب هشدارهای تولید شده نیز مربوط به اعمالِ مُجازی می‌باشند که یک مخاطره‌ی امنیتی واقعی را دربرندارند، در نتیجه ممکن است با توجه به تَعدد هشدارها، سطح پایین بودن نسبیِ آن‌ها و نادرست بودن بخش عمده‌ای از آن‌ها، مدیرسیستم پس از مدتی نسبت به هشدارهای تولید شده بی‌توجه شود. روشن است که این مشکل عملا IDS را بی‌فایده می‌کند و فلسفه‌ی وجود آن‌را زیر سوال می‌برد.

معمولا برای حلِ این مشکل از یک واحدِ مدیریت هشدارها استفاده می‌شود. این واحد با پردازش هشدارها تعداد آن‌ها را کاهش‌داده و سطح معنایی هشدارهای تولیدی را نیز بالا می‌برد. به مجموعه‌ی اعمالی که در واحد مدیریت هشدارها انجام می‌شود همبسته‌سازی هشدارها[1] گفته می‌شود. ورودیِ این واحد جریانی از هشدارهای به ظاهر غیر‌مرتبط و پردازشِ انجام‌شده در آن، یافتنِ ارتباطات بین این هشدارها و همبسته‌سازی آن‌ها است. سیستم همبسته‌ساز با ارائه‌ی یک یا چند سناریوی سطحِ بالا که از توالی و مرتبط‌شدن هشدارهای ورودی ایجاد شده‌اند و می‌توانند یک حمله‌ی مشخص را نشان‌دهند، سطحِ معنایی هشدارها را بالا می‌برد. به این‌ترتیب یک دید کلی و همه‌جانبه نسبت به وضعیت امنیتی موجود بدست می‌آید. هشدارهای سطحِ پایین ممکن‌است خروجی اجزاءِ مختلفِ یک IDS باشند که نشان‌دهنده‌ی رویدادهای مختلفی است که توسط IDS مشاهده شده‌است و بایستی این رویدادها به هم مرتبط‌شوند و یا ممکن‌است ناشی از فعالیت چندین IDS موجود در شبکه باشد (معمولا در این حالت به هر یک از این IDSها حسگر[2] گفته می‌شود). به‌هر حال در هر دو صورت عمل همبسته‌سازی، رویدادها و یا هشدارها را با یکدیگر مرتبط نموده و اعلام خطر می‌نماید و مدیر سیستم نیز به‌جای دریافت نشانه‌های ضعیف، متعدد و پراکنده‌ی خطر تعداد کمتری هشدار سطح بالا و تجمیع شده‌ی معنی‌دار را دریافت می‌کند.

با توجه به اهمیت IDS در بهبود وضعیت امنیتی یک شبکه‌ی کامپیوتری و با توجه به مشکل مطرح شده پیرامون هشدارهای تولید شده توسط آن، روشن است که عمل همبسته‌سازی هشدارها نیز بسیارحائز اهمیت خواهد بود. با توجه به اهمیتِ این عمل، روش‌های متعددی برای برخورد با آن پیشنهاد شده‌است. برای دستیابی به اهداف همبسته-

---

[1] Alert Correlation
[2] Sensor

سازی، روشهای مبتنی بر همجوشیِ هشدارها با استفاده از معیارهای شباهت، هشدارهای تکراری را به یکدیگر پیوند داده و یک هشدار کلی برای آنها تولید می‌کنند. روشن است که با کم شدن تعداد هشدارها بخشی از هدف همبسته-سازی تامین می‌شود. روش‌های مبتنی بر فیلترکردنِ هشدارها با استفاده از اطلاعات زمینه‌ایِ ازپیش جمع‌آوری شده و ذخیره‌شده، سعی می‌کنند هشدارهای نادرست را فیلتر کرده و دور بریزند. با انجام این کار نیز تعداد هشدارهایی که مدیر امنیتی سیستم دریافت می‌کند کاهش می‌یابد و در نتیجه بخش دیگری از اهداف همبسته‌سازی تامین می‌شود. هرچند دو روش همبسته‌سازی مبتنی بر همجوشی و مبتنی بر فیلتر تعداد هشدارها را کم می‌کنند اما باعث افزایش سطح معنایی هشدارها نمی‌شوند. یعنی با استفاده از آن‌ها مدیر سیستم فقط تعداد کمتری از هشدارهای پراکنده‌ی بدون ارتباط سببی را دریافت می‌کند. روش‌های مبتنی بر استخراجِ روابطِ سببیِ بین هشدارها، سعی در حل این بخش از مشکل همبسته‌سازی دارند. این روش‌ها به توالی، ترتیب و همزمانی هشدارها توجه می‌کنند تا سناریوهای حملات را استخراج و به تولید هشدارهای سطح بالا بپردازند. برای این‌کار نیز یا صریحا دانشِ متخصصینِ حملاتِ کامپیوتری پیرامونِ ترتیب و توالیِ مراحلِ یک حمله‌ی خاص را کُدکرده و در پایگاه دانش خود ذخیره می‌کنند و یا از روش-های آماری و یادگیری ماشینی برای استخراج این ترتیب و توالی استفاده می‌کنند.

هریک از سه گروه روش‌های معرفی‌شده، بخشی از مشکلاتی که مدیر سیستم در برخورد با هشدارهای تولید شده توسط یک یا چند IDS با آن‌ها روبرو است را حل می‌کنند. اما هریک از این روش‌ها نیز کاستی‌ها و مشکلات خاص خود را دارند. عدم توانایی در استخراج روابط سببی، نیاز به جمع‌آوری اطلاعات زمینه‌ای مربوط به شبکه و کاربران، نیاز به تعریف روابط سببی بین هشدارها، وابستگی به دانشِ متخصصینِ حملات کامپیوتری، عدم توانایی در مقابله با حملات جدید، نیاز برای بروز کردن اطلاعات ذخیره شده با تغییر پیکربندی شبکه و یا با پیدایش حملات جدید و بار پردازشی بالا و عدم امکان استفاده‌ی برخط تنها بخشی از مشکلاتی است که هریک از این روش‌ها با آن مواجهند.

برای کم‌کردن مشکلات مطرح شده می‌توان از معماری‌های ترکیبی استفاده کرد. این معماری‌ها سعی بر آن دارند تا ضمن برخورداری از مزایای هر یک از روش‌های همبسته‌سازی از کاستی‌های آن‌ها نیز احتراز کنند. روشن است که چالش عمده‌ای که در اینجا مطرح می‌شود ارائه‌ی یک معماری ترکیبی است که چنین هدفی را تامین نماید.

هدف پژوهش

هدف از انجام پژوهش حاضر ارائه‌ی یک روش همبسته‌سازی ترکیبی است که در عین آنکه از دقت کافی در همبسته‌سازیِ هشدارهای مرتبط برخوردار است این‌کار را با چنان کارایی انجام دهد که بارمحاسباتی سیستم نیز

غیرقابل تحمل نشود. علاوه بر آن تا حد امکان از دانش متخصصین حملاتِ کامپیوتری و کُدکردن این دانش نیز بی-نیاز باشد و همچنین حداقل وابستگی را به نمونه‌های خاص حملات داشته‌باشد تا بتواند با پویایی کامل به شناسایی و همبسته‌سازی مراحل مختلف یک حمله‌ی جدید نیز اقدام ورزد و در انجام این‌کار نیز از دقتی قابل رقابت با روش-های ایستای وابسته به حمله برخوردار باشد. روشن است که دستیابی همزمان به دقت، کارایی و پویایی هدفی ستودنی است که دست یافتن به آن مستلزم فرآیندی پیچیده خواهد بود.

روش انجام

روشی که برای دستیابی به اهداف فوق مورد استفاده قرار گرفته است الهام گرفتن از طبیعت برای ساخت یک الگویِ ترکیبیِ پویا، دقیق و کارا می‌باشد. سیستم ایمنی بدن جانداران سیستمی است که وظیفه‌ی پاسداری از بدن را در برابر عوامل بیماری‌زا بعهده‌دارد. با توجه به توانایی‌های منحصربفرد سیستم ایمنی در مقابله با تعداد نامحدودی از عوامل بیماری‌زای شناخته‌شده و ناشناخته، روش کار این سیستم منبع الهامی برای حل بسیاری از مسایل محاسباتی در طی سال‌های اخیر شده‌است. به‌گونه‌ای که مجموعه‌ای از الگوریتم‌ها و روش‌ها تحت عنوان سیستم ایمنی مصنوعی[1] معرفی شده‌است. ساختار لایه‌ای سیستم ایمنی که به طور پویا و با کارایی و دقت وظائف خود را انجام می‌دهد نیز یک ساختار ترکیبی است و راز توانایی سیستم ایمنی در دسترسیِ همزمان به پویایی، دقت و کارایی نیز همین ساختار لایه‌ای است. لذا دور از ذهن نیست که الگوی ساختاریِ لایه‌ای سیستم ایمنی بتواند منجر به تولید یک همبسته‌ساز ترکیبی شود که اهداف مورد نظر ما در همبسته‌سازی را تامین نماید.

فرضیات پژوهش

فرضیه اساسی مطرح شده در این پژوهش آن است که بکارگیری الگوریتمها، روشها، خصوصیات و عناصر موجود در سیستم ایمنی می‌تواند منجر به معرفی یک سیستم همبسته‌سازیِ ترکیبی بهینه شود. لذا با الهام گرفتن از سیستم ایمنی در انتخاب مناسب الگوریتمها، روشها، خصوصیات و عناصر، بهبود در کارکرد سیستم همبسته‌ساز را بررسی می‌نمائیم. برای این منظور یافتن پاسخ هریک از سوالات زیر می‌تواند راهگشا باشد.

- آیا دستیابی همزمان به دقت، کارایی و پویایی از طریق یک سیستم ترکیبی امکان‌پذیر هست؟
- آیا ساختار لایه‌ای سیستم ایمنی می‌تواند منبع الهامی برای طراحی یک همبسته‌ساز ترکیبی باشد؟
- آیا با بکارگیری سیستم ایمنی مصنوعی می‌توان یک سیستم همبسته‌سازی پویا ایجاد کرد؟

---

[1] Artificial Immune System