

بسم الله الرحمن الرحيم



دانشگاه اصفهان

دانشکده فنی و مهندسی

گروه مهندسی کامپیوتر

پایان نامه‌ی دکتری رشته‌ی مهندسی کامپیوتر گرایش نرم افزار

همبسته سازی هشدارها به کمک سیستم ایمنی مصنوعی

استاد راهنما:

دکتر احمد برآنی دستجردی

استاد مشاور:

دکتر عباس رضائی

پژوهشگر:

مهدی باطنی

مهر ماه ۱۳۹۱

کلیه‌ی حقوق مادی مترتب بر نتایج مطالعات،
ابتکارات و نوآوری‌های ناشی از تحقیقِ موضوعِ این
پایان‌نامه متعلق به دانشگاه اصفهان است



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 ۱۱/۰۷/۹۱ توسط هیأت داوران زیر بررسی و با درجه ... (ب.ا.ب.) ... به تصویب نهایی رسید.

امضا

۱- استاد/ استادان راهنمای پایان نامه دکتر ... احمد برآنی ... با مرتبه‌ی علمی ... دانشیار ...

امضا

۲- استاد/ استادان مشاور پایان نامه دکتر ... عباس رضائی ... با مرتبه‌ی علمی ... استاد ...

امضا

۳- استاد/ استادان داور داخل گروه دکتر ... کامران زمانی فر ... 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 ...

امضای مدیر گروه

سپاسگذاری:

در اینجا بر خود لازم می‌دانم مراتب سپاس خود را به پیشگاه کلیه اساتیدی که در طی این دوره پژوهشی از دانش آنها بهره گرفته‌ام تقدیم دارم. بویژه استاد محترم راهنمایم جناب آقای دکتر احمد برآنی 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 نیوبرنسیویک کانادا که در طی دوران فرصت مطالعاتی از دانش و تجربیاتشان به وفور بهره‌بردم صمیمانه سپاسگذاری می‌نمایم.

این پایان نامه پیشکشی است ناچیز به رسم قدردانی به تمامی آنها که برایم عزیزند، پدر و مادر بزرگوام که با تمام توان از ابتدایی ترین دوران دانش اندوزی تا امروز همیشه مشوق و پشتیبان من بوده اند، همسر مهربانم که در تمام دوران پر فراز و نشیب تحصیلات دکتری در تمامی سختی ها یار و یاور من بوده است و دستیابی به این هدف سترگ بدون پشتیبانی های او میسر نمی شد و تمامی اساتید و آموزگاران که در مقاطع مختلف تحصیلی از دانش و فضائل اخلاقی آنها بهره برده ام.

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 نخواهد بود. شناخته‌شده‌ترین راه‌حل برای مواجهه با مشکل تعداد زیاد هشدارها، همبسته‌کردن آنهاست. 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 حملات 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 کلی 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 هر یک 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 معماری ترکیبی سه لایه به نام 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. معماری 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 یکی از الگوریتمهای شناخته‌شده‌ی سیستم ایمنی مصنوعی به نام AIRS برای یادگیری با نظارت استفاده می‌کند. معماری سه‌لایه‌ی iCorrelator از ترکیبی از دانش اولیه‌ی محدود در قالب قوانین عمومی غیر وابسته به حملات خاص برای مواجهه با حالات پیش‌بینی شده، یک الگوریتم یادگیری بانظارت برای مواجهه با حالات جدید و پیش‌بینی نشده و همچنین سلولهای حافظه‌ی ایمنی برای بخاطر سپردن این حالات جدید برای مواجهه‌های بعدی استفاده می‌کند. هدف از بکارگیری این ساختار ترکیبی سه‌لایه در iCorrelator برخورداری از دقت در عین کارایی و پویایی می‌باشد. مجموعه‌های داده‌ای DRPA2000 و netForensics honeynet برای بررسی دقت و کارایی iCorrelator مورد استفاده قرار گرفته‌اند. سه معیار کمال، درستی و نرخ‌خطا در همبسته‌سازی برای بررسی دقت و همچنین زمان اجرا برای بررسی کارایی iCorrelator مورد استفاده قرار گرفته‌است. برای کلیه‌ی داده‌های مورد استفاده، iCorrelator توانسته است به صورت پویا و بدون داشتن دانش اولیه‌ی 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 قوانین 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 هیچ‌گونه اطلاع قبلی از کیفیت وقوع آنها ندارد و ارائه‌ی گراف حمله‌ی آنها، شاهده‌ی بر صحت عملکرد پویای آن می‌باشد.

واژگان کلیدی:

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

فهرست مطالب

صفحه	عنوان
۱	فصل اول: معرفی
۷	فصل دوم: ادبیات موضوع
۸	۱-۲- سیستمهای تشخیص نفوذ
۱۴	۲-۲- مدیریت هشدارها و فرآیند همبسته‌سازی
۱۴	۱-۲-۲ فرآیند همبسته‌سازی
۱۹	۳-۲- آشنایی با سیستم ایمنی مصنوعی
۲۰	۱-۳-۲ سیستم ایمنی طبیعی
۲۴	۲-۳-۲- الگوریتم‌های سیستم ایمنی مصنوعی
۲۵	۴-۲- جمع‌بندی
۲۶	فصل سوم: پیشینه‌ی تحقیق
۲۷	۱-۳- همبسته‌سازی هشدارها
۲۷	۱-۱-۳- همبسته‌سازی مبتنی بر همجوشی
۳۰	۲-۱-۳- همبسته‌سازی مبتنی بر فیلتر
۳۲	۳-۱-۳- مبتنی همبسته‌سازی بر روابط سببی
۴۱	۴-۱-۳- چارچوب جامع همبسته‌سازی
۴۳	۲-۳- سیستم‌های تشخیص نفوذ و سیستم ایمنی مصنوعی

عنوان	صفحه
۳-۳- همبسته‌سازی هشدارها و سیستم ایمنی مصنوعی	۴۶
۳-۴- جمع‌بندی	۴۸
فصل چهارم: انطباق دهنده‌ی قوانین فازی و لایه‌ی اول همبسته‌سازی در iCorrelator	
۴-۱- معماری iCorrelator برای همبسته‌سازی هشدارها	۵۰
۴-۲- لایه‌ی اول همبسته‌سازی، همبسته‌سازی مبتنی بر قانون	۵۷
۴-۲-۱- سیستم ایمنی ذاتی	۵۷
۴-۲-۲- ماتریس‌های نگهداری داده‌های همبسته‌سازی	۵۸
۴-۲-۳- واحد مولد سلول‌ها	۶۱
۴-۲-۴- داده‌های آموزشی	۶۵
۴-۲-۵- قوانین فازی	۶۸
۴-۲-۶- تطبیق دهنده‌ی فازی	۶۹
۴-۲-۷- فراهشدارها و فرآیند همبسته‌سازی در لایه‌ی اول	۷۴
۴-۳- جمع‌بندی	۷۶
فصل پنجم: الگوریتم سیستم تشخیص ایمنی مصنوعی و لایه‌ی دوم همبسته‌سازی در iCorrelator	
۵-۱- پاسخ اولیه در سیستم ایمنی اکتسابی	۷۸
۵-۲- الگوریتم سیستم تشخیص ایمنی مصنوعی	۷۸
۵-۲-۱- مراحل اجرایی الگوریتم AIRS	۸۳
۵-۳- الگوریتم سیستم تشخیص ایمنی مصنوعی توسعه یافته	۸۷

عنوان	صفحه
۱-۳-۵- وزن‌دهی به ویژگی‌ها	۸۸
۲-۳-۵- سیاست انتخاب کلاس	۹۴
۳-۳-۵- تبدیل شماره‌ی کلاس به احتمال	۹۴
۴-۵- ارتباط لایه‌ی دوم با لایه‌ی اول در فرآیند همبسته‌سازی	۹۸
۵-۵- جمع‌بندی	۹۸
فصل ششم: لایه سوم همبسته‌سازی - سلول‌های حافظه‌ی ایمنی و سایر اجزاء iCorrelator	
۱-۶- پاسخ ثانویه در سیستم ایمنی اکتسابی	۱۰۰
۲-۶- سلول‌های حافظه و انطباق دهنده‌ی اقلیدسی سلول‌ها	۱۰۱
۳-۶- ارتباط لایه‌ی سوم با سایر لایه‌ها و فرآیند همبسته‌سازی	۱۰۳
۴-۶- سیاست‌گذاری انتخاب هشدارها	۱۰۷
۱-۴-۶- سیاست انتخاب همه‌ی هشدارها	۱۰۷
۲-۴-۶- سیاست مبتنی بر پنجره‌ی زمانی	۱۰۸
۳-۴-۶- سیاست مبتنی بر پنجره‌ی زمانی تصادفی	۱۰۸
۴-۴-۶- سیاست مبتنی بر پنجره‌ی زمانی تصادفی جهت‌دار	۱۱۱
۵-۶- مولد گراف حمله	۱۱۴
۶-۶- تحلیل کارایی iCorrelator	۱۱۶
۷-۶- جمع‌بندی	۱۱۸
فصل هفتم: پیاده‌سازی، ارزیابی و بررسی نتایج	
	۱۲۰

عنوان	صفحه
۱-۷- پیاده‌سازی iCorrelator	۱۲۰
۲-۷- مجموعه‌های داده‌ای مورد استفاده	۱۲۲
۱-۲-۷- مجموعه‌ی داده‌ای DARPA2000	۱۲۳
۲-۲-۷- مجموعه‌ی داده‌ای netForensics Honeynet	۱۲۳
۳-۷- معیارهای ارزیابی	۱۲۴
۱-۳-۷- ارزیابی دقت	۱۲۴
۲-۳-۷- ارزیابی کارایی	۱۲۷
۴-۷- بررسی نتایج	۱۲۷
۱-۴-۷- iCorrelator و حمله‌ی LLDoS1.0	۱۲۸
۲-۴-۷- iCorrelator و حمله‌ی LLDoS2.0	۱۳۵
۳-۴-۷- iCorrelator و حمله‌ی موجود در داده‌های Honeynet	۱۳۹
۵-۷- بررسی تاثیر پارامترها بر عملکرد iCorrelator	۱۴۷
۶-۷- جمع‌بندی	۱۵۵
فصل هشتم: نتیجه‌گیری و راهکارهای آینده	۱۵۶
۱-۸- نتیجه‌گیری	۱۵۶
۲-۸- راهکارهای آینده	۱۶۳
پیوست‌ها	۱۶۶
۱- پیوست ۱- سناریوی حمله‌ی LLDoS1.0	۱۶۶

عنوان

صفحه

پیوست ۲- سناریوی حمله‌ی LLDoS2.0 ۱۶۹

منابع و مآخذ ۱۷۲

فهرست شکلها

عنوان	صفحه
شکل ۱-۲- ویژگیهای سیستمهای تشخیص نفوذ	۹
شکل ۲-۲- طبقه‌بندی روشهای تشخیص ناهنجاری	۱۱
شکل ۳-۲- طبقه‌بندی سیستمهای تشخیص نفوذ بر اساس روش‌های بکاررفته	۱۱
شکل ۴-۲- طبقه‌بندی IDS ها بر اساس محل استقرار و منابع اطلاعاتی	۱۲
شکل ۵-۲- طبقه‌بندی بر اساس نحوه توزیع حسگرها	۱۲
شکل ۶-۲- طبقه‌بندی بر اساس معماری	۱۳
شکل ۷-۲- سیستم‌های تشخیص نفوذ مبتنی بر داده کاوی	۱۳
شکل ۸-۲- مراحل فرآیند همبسته‌سازی هشدارها	۱۶
شکل ۹-۲- الف- یک لنفوسیت T در انسان	۲۱
شکل ۹-۲- ب- تطابق رسپتورها و اپیتوپ‌ها در خلال تشخیص	۲۱
شکل ۱۰-۲- فرآیند تشخیص، تکثیر، تولید آنتی‌بادی و تولید سلولهای حافظه	۲۲
شکل ۱-۳- مولفه‌های پیشنهادی برای فرآیند همبسته‌سازی هشدارها	۴۲
شکل ۱-۴- مقایسه‌ی iCorrelator با سیستم‌ایمنی بدن انسان	۵۱
شکل ۲-۴- معماری iCorrelator	۵۲
شکل ۳-۴- ماتریس همبستگی هشدارها	۵۹
شکل ۴-۴- تولید یک سلول از دو هشدار ورودی	۶۲

عنوان	صفحه
شکل ۴-۵- توابع عضویت برای هر یک از واژگان فازی بکار رفته	۷۱
شکل ۵-۱- روندنمای ساده شده‌ی الگوریتم AIRS	۸۱
شکل ۵-۲- یک مجموعه‌ی داده‌ای شامل n بردار هر یک شامل m ویژگی و یک مقدار عددی	۹۲
شکل ۵-۳- وزنهای تولید شده توسط روش متوسط مشارکت برای شش ویژگی مورد استفاده	۹۳
شکل ۵-۴- تعیین کلاس برنده بر اساس میانگین فاصله عناصر	۹۴
شکل ۶-۱- نحوه‌ی جستجوی سلولها در حافظه‌ی ایمنی	۱۰۳
شکل ۶-۲- نحوه‌ی نگهداری فراهشدارها و هشدارهای آنها در حافظه‌ی اصلی	۱۰۴
شکل ۶-۳- یک پنجره‌ی زمانی با پنج شکاف زمانی و تعداد هشدارهای هر شکاف	۱۰۹
شکل ۶-۴- تعداد هشدارهای انتخابی در دو سیاست انتخاب تصادفی و تصادفی جهتدار برای inside2	۱۱۳
شکل ۷-۱- نمایی از iCorrelator و گراف حمله‌ی استخراج شده برای مجموعه هشدارهای Inside1	۱۲۲
شکل ۷-۲- نمایش مفاهیم تمامیت، رسایی و نرخ خطا در همبسته‌سازی	۱۲۶
شکل ۷-۳- یکی از فراهشدارهای استخراج شده از هشدارهای Inside1 برای حمله‌ی LLDoS1.0	۱۲۹
شکل ۷-۴- گراف‌های حمله‌ی استخراج شده از Inside1	۱۳۰
شکل ۷-۵- ارزیابی دقت برای داده‌های Inside1	۱۳۴
شکل ۷-۶- یکی از فراهشدارهای استخراج شده از هشدارهای Inside2 برای حمله‌ی LLDoS2.0	۱۳۵
شکل ۷-۷- گراف‌های حمله‌ی استخراج شده از Inside2	۱۳۶
شکل ۷-۸- ارزیابی دقت برای داده‌های Inside2	۱۴۰
شکل ۷-۹- بخشی از فراهشدار استخراج شده از داده‌های Honeynet استخراج شده از ترافیک روز دوم	۱۴۲

- شکل ۷-۱۰- گراف‌های حمله‌ی استخراج شده از Honeynet ۱۴۳
- شکل ۷-۱۱- ارزیابی کارایی iCorrelator ۱۴۶
- شکل ۷-۱۲- رابطه‌ی تمامیت، رسایی و نرخ خطا در همبسته‌سازی با تعداد سلولها ۱۴۸
- شکل ۷-۱۳- تعداد هشدارهای انتخاب شده در همبسته‌سازی هشدارهای Inside1 ۱۴۹
- شکل ۷-۱۴- تعداد هشدارهای انتخاب شده برای پنجره‌های زمانی مختلف با سیاست انتخاب تصادفی جهتدار ۱۵۰
- شکل ۷-۱۵- مقایسه‌ی زمان اجرا با پنجره‌های زمانی مختلف با سیاست RDTW برای netForensics ۱۵۲
- شکل ۷-۱۶- تعداد هشدارهای همبسته‌شده برای داده‌های inside2 در هر یک از سه‌لایه ۱۵۴

فهرست جدول‌ها

صفحه	عنوان
۱۵.....	جدول ۱-۲- مقایسه‌ی اجزا یک سیستم همبسته‌سازی
۶۷.....	جدول ۱-۴- داده‌های آموزشی برای بیان روابط همبسته‌سازی و احتمال همبسته‌سازی
۶۸.....	جدول ۲-۴- قوانین مورد استفاده در لایه‌ی مبتنی بر قوانین
۷۹.....	جدول ۱-۵- مقایسه‌ی دقت AIRS با LVQ برای تعداد مختلف ویژگیها
۸۳.....	جدول ۲-۵- نمونه‌هایی از سلولهای حافظه‌ی تولید شده توسط AIRS
۱۱۸.....	جدول ۱-۶- مقایسه‌ی سیاست‌های مختلف انتخاب هشدار از نظر زمان و حافظه‌ی مصرفی
۱۲۱.....	جدول ۱-۷- مقایسه‌ی نتایج تولیدی توسط سه پیاده‌سازی AIRS
۱۲۸.....	جدول ۲-۷- پارامترهای استفاده شده در ارزیابی iCorrelator
۱۳۱.....	جدول ۳-۷- مقایسه‌ی دقت iCorrelator بر روی هشدارهای Inside1 با چند کار مشابه
۱۳۲ ..	جدول ۴-۷- مقایسه‌ی ۳ معیار دقت و زمان اجرا با سیاست‌های مختلف و تعداد لایه‌های مختلف برای Inside1
۱۳۷.....	جدول ۵-۷- مقایسه‌ی دقت iCorrelator بر روی هشدارهای Inside2 با چند کار مشابه
۱۳۸ ..	جدول ۶-۷- مقایسه‌ی ۳ معیار دقت و زمان اجرا با سیاست‌های مختلف و تعداد لایه‌های مختلف برای Inside2
۱۴۱.....	جدول ۷-۷- هشدارهایی موجود در سناریوی کامل حمله‌ی موجود در داده‌های Honeynet
۱۴۵.....	جدول ۸-۷- مقایسه‌ی ۳ معیار دقت و زمان اجرا با سیاست‌های مختلف برای Honeynet
۱۵۱.....	جدول ۹-۷- مقایسه‌ی زمان اجرا با پنجره‌های زمانی مختلف با سیاست RDTW برای netForensics

فصل اول

معرفی

با توجه به گسترش استفاده از شبکه‌های کامپیوتری و کاربرد فراگیر آن در مدیریت جنبه‌های مختلف زندگی امروزی، اهمیت تامین امنیت اطلاعات نگهداری شده و مبادله شده روزبه‌روز بیشتر آشکار می‌شود. به گونه‌ای که امنیت اطلاعات در مبادلات الکترونیکی یکی از مهمترین دغدغه‌های فکری کاربران برای استفاده یا عدم استفاده از سیستم‌های کامپیوتری است. امنیت اطلاعات دارای جنبه‌های مختلفی است بر همین اساس ابزارها و روش‌های مختلفی برای تامین جنبه‌های مختلف امنیت پیش‌بینی شده است. روش‌های رمزنگاری، پروتکل‌های امنیتی، کنترل دسترسی، آنتی‌ویروس‌ها، دیوارهای آتش و سیستم‌های تشخیص نفوذ¹ هر یک در سطحی با تامین امنیت اطلاعات سروکار دارند. با توجه به اینکه امکان تعریف همه‌ی اعمال غیرمجاز در یک سیستم و یا شبکه‌ی کامپیوتری وجود ندارد و از طرفی اعمالی وجود دارند که بخودی‌خود مجاز هستند اما از ترکیب آن‌ها می‌توان یک هدف غیرمجاز را عملی کرد لذا دامنه‌ی اعمال محدودیت بر توانایی‌های کاربران، معمولاً دارای محدودیت می‌شود. در این بین سیستم‌های تشخیص نفوذ (IDS) به بررسی رفتارهای کاربران یک سیستم یا یک شبکه‌ی کامپیوتری می‌پردازند تا سوءاستفاده‌های احتمالی کاربران را از اعمالی که مجاز به انجام آن هستند شناسایی و گزارش نمایند. به این ترتیب IDS به یکی از اجزاء اساسی امنیتی در سیستم‌های کامپیوتری تبدیل شده است 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 زیادی هشدارها و کم‌اهمیت بودن نسبی هر یک از آن‌ها، شناسایی مخاطرات امنیتی و تصمیم‌گیری درست در مورد آن‌ها برای مدیر سیستم بسیار مشکل خواهد بود. علاوه بر این اغلب هشدارهای تولید شده نیز مربوط به اعمال مجازی می‌باشند که یک مخاطره‌ی امنیتی واقعی را دربر ندارند، در نتیجه ممکن است با توجه به تعدد هشدارها، سطح پایین بودن نسبی آن‌ها و نادرست بودن بخش عمده‌ای از آن‌ها، مدیر سیستم پس از مدتی نسبت به هشدارهای تولید شده بی‌توجه شود. روشن است که این مشکل عملا IDS را بی‌فایده می‌کند و فلسفه‌ی وجود آن را زیر سوال می‌برد.

معمولا برای حل این مشکل از یک واحد مدیریت هشدارها استفاده می‌شود. این واحد با پردازش هشدارها تعداد آن‌ها را کاهش داده و سطح معنایی هشدارهای تولیدی را نیز بالا می‌برد. به مجموعه‌ی اعمالی که در واحد مدیریت هشدارها انجام می‌شود همبسته‌سازی هشدارها^۱ گفته می‌شود. ورودی این واحد جریانی از هشدارهای به ظاهر غیر-مرتبط و پردازش انجام شده در آن، یافتن ارتباطات بین این هشدارها و همبسته‌سازی آن‌ها است. سیستم همبسته‌ساز با ارائه‌ی یک یا چند سناریوی سطح بالا که از توالی و مرتبط شدن هشدارهای ورودی ایجاد شده‌اند و می‌توانند یک حمله‌ی مشخص را نشان دهند، سطح معنایی هشدارها را بالا می‌برد. به این ترتیب یک دید کلی و همه‌جانبه نسبت به وضعیت امنیتی موجود بدست می‌آید. هشدارهای سطح پایین ممکن است خروجی اجزای مختلف یک IDS باشند که نشان‌دهنده‌ی رویدادهای مختلفی است که توسط IDS مشاهده شده‌است و بایستی این رویدادها به هم مرتبط شوند و یا ممکن است ناشی از فعالیت چندین IDS موجود در شبکه باشد (معمولا در این حالت به هر یک از این IDSها حسگر^۲ گفته می‌شود). به هر حال در هر دو صورت عمل همبسته‌سازی، رویدادها و یا هشدارها را با یکدیگر مرتبط نموده و اعلام خطر می‌نماید و مدیر سیستم نیز به جای 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 بسیار حائز اهمیت خواهد بود. با توجه به اهمیت این عمل، روش‌های متعددی برای برخورد با آن پیشنهاد شده‌است. برای دستیابی به اهداف همبسته-

¹ Alert Correlation

² Sensor

سازی، روشهای مبتنی بر همجوشی هشدارها با استفاده از معیارهای شباهت، هشدارهای تکراری را به یکدیگر پیوند داده و یک هشدار کلی برای آنها تولید می کنند. روشن است که با کم شدن تعداد هشدارها بخشی از هدف همبسته-سازی تامین می شود. روش های مبتنی بر فیلتر کردن هشدارها با استفاده از اطلاعات زمینه ای از پیش جمع آوری شده و ذخیره شده، سعی می کنند هشدارهای نادرست را فیلتر کرده و دور بریزند. با انجام این کار نیز تعداد هشدارهایی که مدیر امنیتی سیستم دریافت می کند کاهش می یابد و در نتیجه بخش دیگری از اهداف همبسته سازی تامین می شود. هرچند دو روش همبسته سازی مبتنی بر همجوشی و مبتنی بر فیلتر تعداد هشدارها را کم می کنند اما باعث افزایش سطح معنایی هشدارها نمی شوند. یعنی با استفاده از آنها مدیر سیستم فقط تعداد کمتری از هشدارهای پراکنده بدون ارتباط سببی را دریافت می کند. روش های مبتنی بر استخراج روابط سببی بین هشدارها، سعی در حل این بخش از مشکل همبسته سازی دارند. این روش ها به توالی، ترتیب و همزمانی هشدارها توجه می کنند تا سناریوهای حملات را استخراج و به تولید هشدارهای سطح بالا بپردازند. برای این کار نیز یا صریحا دانش متخصصین حملات کامپیوتری پیرامون ترتیب و توالی مراحل یک حمله ی خاص را گد کرده و در پایگاه دانش خود ذخیره می کنند و یا از روش های آماری و یادگیری ماشینی برای استخراج این ترتیب و توالی استفاده می کنند.

هریک از سه گروه روش های معرفی شده، بخشی از مشکلاتی که مدیر سیستم در برخورد با هشدارهای تولید شده توسط یک یا چند IDS با آنها روبرو است را حل می کنند. اما هریک از این روش ها نیز کاستی ها و مشکلات خاص خود را دارند. عدم توانایی در استخراج روابط سببی، نیاز به جمع آوری اطلاعات زمینه ای مربوط به شبکه و کاربران، نیاز به تعریف روابط سببی بین هشدارها، وابستگی به دانش متخصصین 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 استفاده ی برخط تنها بخشی از مشکلاتی است که هریک از این روش ها با آن مواجهند.

برای کم کردن مشکلات مطرح شده می توان از معماری های ترکیبی استفاده کرد. این معماری ها سعی بر آن دارند تا ضمن برخورداری از مزایای هر یک از روش های همبسته سازی از کاستی های آنها نیز احتراز کنند. روشن است که چالش عمده ای که در اینجا مطرح می شود ارائه ی یک معماری ترکیبی است که چنین هدفی را تامین نماید.

هدف پژوهش

هدف از انجام پژوهش حاضر ارائه ی یک روش همبسته سازی ترکیبی است که در عین آنکه از دقت کافی در همبسته سازی هشدارهای مرتبط برخوردار است این کار را با چنان کارایی انجام دهد که بار محاسباتی سیستم نیز

غیرقابل تحمل نشود. علاوه بر آن تا حد امکان از دانش متخصصین حملات کامپیوتری و کُد کردن 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 این کار 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 الگوی ترکیبی 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 منحصر بفرد 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. به گونه‌ای که مجموعه‌ای از الگوریتم‌ها و روش‌ها تحت عنوان سیستم ایمنی مصنوعی^۱ 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 دسترسی همزمان به پویایی، دقت و کارایی نیز همین ساختار لایه‌ای است. لذا دور از ذهن نیست که الگوی ساختاری 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 همبسته‌سازی 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 امکان پذیر 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