
بسم الله الرحمن الرحیم
الحمد لله رب العالمین الرحمن الرحیم مالک یوم الدین
ایاک نعبد و ایاک نستعین اهدنا الصراط المستقیم
صراط الذین انعمت علیهم غیر المغضوب علیهم
ولا الضالین

دانشگاه الزهرا (س)

دانشکده فنی و مهندسی

پایان نامه

جهت اخذ درجه کارشناسی ارشد

رشته مهندسی کامپیوتر - گرایش هوش مصنوعی

عنوان

ارائه ی یک سیستم تشخیص نفوذ هوشمند، مبتنی بر رویکرد ماشین مجازی

استاد راهنما

دکتر رضا عزمی

دانشجو

بشری پیشگو

اسفند ماه سال ۱۳۹۰

کلیه دستاوردهای این تحقیق متعلق به دانشگاه الزهرا (س) می‌باشد.

تقدیم

تقدیم به همه‌ی تجلیل‌گرانی که هنر و هنرمندان را ارزش می‌دانند.

به پاس تعهد بی‌دریغ انسان‌هایی که از کلمه ایثار

و به پاس محبت‌های بی‌دریغشان که هرگز پایان نمی‌پذیرد

این مجموعه را به پدر عزیزم تقدیم می‌کنم

قدردانی

ای خدایی که به ما نعمت اندیشیدن و توانایی آموختن عطا فرمودی و با تجهیز آدمی به این دو نیرو، او را اشرف مخلوقات خود به لطف خود گردانیدی، اراده کردم تا در مسیر کسب علم و دانش قدم بگذارم و در سایه‌ی الطاف امیرالمؤمنین علی علیه السلام و به دعای خیر پدر و مادر مهربانم در این طریق یاری‌ام بخشیدی و پژوهش و یادگیری را در قلبم نهادینه فرمودی و استادی گرانقدر اندیشمند و خلاق چون دکتر رضا عزمی به راهنمایی‌ام گمارد که اندیشه‌های نیکو و برکات و چراغ راه پژوهشم گردد.

پروردگارا، با تمام عشق و اشتیاق تمام یکایک نعمت‌هایت را که با رحمت به من عطا فرمودی و یا به حکمت از من دریغ داشتی، سپاس می‌گویم و ستایشت می‌کنم که تو به حق شایسته ستایشی.

چکیده

یکی از چالش‌های اساسی در مبحث امنیت سیستم‌های کامپیوتری، تشخیص فعالیت‌های خرابکارانه و نفوذی به سیستم می‌باشد. به همین جهت تشخیص نفوذ بر پایه‌ی متدهای یادگیری، هم‌اکنون به یکی از رویکردهای فعال در تحقیقات امنیتی تبدیل شده است. این تحقیقات دارای دو چالش عمده می‌باشند. نخست جمع‌آوری امن اطلاعات و دوم ایجاد متدی دقیق برای تشخیص ناهنجاری‌ها. در اینجا ما از فراخوان‌های سیستمی و آرگومان‌های آن‌ها، به عنوان الگویی برای توصیف رفتار فرایندهای سیستمی استفاده می‌نماییم.

در کاربردهای امنیتی، الگوهای رفتاری می‌بایست به صورت کاملا امن و به دور از دستبرد و تغییر مهاجمان و روت‌کیت‌ها جمع‌آوری گردند. به همین منظور، در این پژوهش، سیستمی نوین با عنوان SHADuDT[1] ارائه می‌دهیم. این سیستم در حقیقت نوعی معماری امن و مبتنی بر ناظر[2] است که از یک سو با بکارگیری مؤلفه‌ای تحت عنوان رویدادنگار امن (SHADuDT_SA[3]) به جمع‌آوری امن اطلاعات مرتبط با فراخوان‌های سیستمی در لایه‌ی مانیتور ماشین مجازی می‌پردازد و از سویی دیگر، رفتارهای هنجار و ناهنجار را از طریق متدی تحت عنوان SHADuDT_DM[4] تفکیک می‌نماید. SHADuDT_DM الگوریتمی نوین در حوزه‌ی سیستم‌های ایمنی مصنوعی می‌باشد که از تئوری خطر به عنوان یکی از جدیدترین تئوری‌های ایمنی‌شناسی الهام می‌پذیرد و به شبیه‌سازی همزمان عملکردهای هر دو سیستم ایمنی طبیعی و انطباقی می‌پردازد.

این پژوهش پس از ارائه‌ی معماری SHADuDT، به ارزیابی کارایی آن بر اساس معیارهای گوناگون و نیز مقایسه‌ی SHADuDT_DM با متدهای تشخیص نفوذ کلاسیک در حوزه‌ی سیستم‌های ایمنی مصنوعی می‌پردازد. آزمایشات صورت‌گرفته نشان می‌دهند که معماری امن ارائه‌شده با بهره‌گیری همزمان از مزایای سیستم‌های ایمنی مصنوعی و تکنولوژی ناظر، قادر است با تحمل میزان کمی سربار‌ه‌ی زمانی و حافظه‌ای، به رشد قابل توجهی در دقت تشخیص دست یابد.

واژه‌های کلیدی: تشخیص ناهنجاری، سیستم ایمنی مصنوعی، تئوری خطر، تکنولوژی ناظر

[1] Secure Hypervisor based Anomaly Detection using Danger Theory (SHADuDT)
[2] hypervisor
[3] SHADuDT_Secure Auditor (SHADuDT_SA)
[4] SHADuDT_Detection Method (SHADuDT_DM)

فهرست مطالب

فهرست جداول

فهرست اشکال

فصل اول : مقدمه و هدف پژوهش

۱-۱ مقدمه

یکی از چالش‌های اساسی در مبحث امنیت سیستم‌های کامپیوتری، تشخیص فعالیت‌های خرابکارانه و نفوذی به سیستم می‌باشد. این عملیات نفوذگرانه، صحت[۱]، محرمانگی[۲] و در دسترس بودن[۳] منابع سیستم و شبکه را تهدید می‌نمایند و علیرغم تلاش‌های فراوان در جهت مقابله با آنها، هر روز با شکلی نوین و سیاستی تازه‌تر، اهداف خویش را پی می‌گیرند.

فعالیت‌های نفوذگرانه به سیستم‌های کامپیوتری، از طریق نرم‌افزارهای بدخواه[۴] یا بدافزارها[۵] صورت می‌پذیرد. این بدافزارها که با نیت ورود، اعمال تغییر و یا تخریب دیگر نرم‌افزارهای موجود در کامپیوتر، بدون مجوز وارد آن می‌شوند، انواع متنوعی نظیر ویروس‌ها، کرم‌ها، اسب-های تراوا[۶]، شماره‌گیرها[۷]، درهای پشتی[۸]، نرم‌افزارهای جاسوسی[۹] و روت‌کیت‌ها[۱۰] را شامل می-شوند. رشد پرسرعت این بدافزارها موجب گردیده است که تشخیص و مقابله با آنها یکی از ضروری‌ترین گام‌ها در جهت ایمن‌سازی سیستم‌های کامپیوتری محسوب گردد.

روت‌کیت‌ها یکی از خطرناک‌ترین انواع بدافزارها به حساب می‌آیند که قادر به حفظ حضوری ثابت، استوار و غیرقابل کشف بر روی سیستم بوده و به منظور به خطر انداختن و کنترل سیستم از راه دور، به همراه بیشتر انواع بدافزار بکارگرفته می‌شوند. زمانی که یک روت-کیت، به عنوان کاربر ریشه اجرا می‌شود، می‌تواند به تمامی منابع ماشین تحت نفوذ دسترسی یابد و آنها را به صورت دلخواه تغییر دهد. همین قدرت مطلق روت‌کیت‌ها سبب شده است که دفاع و مقابله با آنها در سال‌های اخیر، به عنوان یکی از چالش برانگیزترین موضوعات در جوامع امنیتی مطرح شود.

در همین راستا، هدف اصلی این پژوهش، ارائه‌ی یک چارچوب مناسب برای تشخیص نفوذ و مقابله با روت‌کیت‌هاست که تا حد امکان قادر به کاهش نواقص و افزایش کارایی سیستم‌های

[1] integrity
[2] confidentiality
[3] availability
[4] Malicious software
[5] Malware
[6] Trojan Horse
[7] dialer
[8] backdoor
[9] Spyware
[10] Rootkit

پیشین باشد. در ادامه، رویکردهای کلیدی این پژوهش را در بخش ۱-۲ و شیوه‌ی سازماندهی مستند را در بخش ۱-۳ بررسی می‌نماییم. در نهایت بخش ۱-۴ خلاصه‌ای از مطالب ذکرشده در این فصل را ارائه می‌دهد.

۱-۲ رویکردهای کلیدی

رویکرد اصلی این پژوهش، ارائه‌ی یک چارچوب مناسب برای تشخیص و مقابله با انواع نفوذ و به ویژه روت‌کیت‌های سطح هسته می‌باشد. ارائه‌ی یک چارچوب جدید در حوزه‌ی سیستم‌های تشخیص نفوذ، نیازمند بررسی دقیق مسائل و چالش‌های گوناگونی نظیر موقعیت قرارگیری این سیستم‌ها و نیز متد تشخیصی مناسب برای کشف نفوذ می‌باشد.

این سیستم‌ها بر اساس موقعیتی که در آن قرار می‌گیرند، به دو دسته‌ی مبتنی بر شبکه و مبتنی بر میزبان تفکیک می‌شوند. سیستم‌های تشخیص نفوذ مبتنی بر شبکه[1] (NIDS) [۵۸]، بر روی کامپیوتر و یا ابزار ویژه‌ای در شبکه قرار می‌گیرند و ترافیک شبکه را به منظور کشف نفوذ، مورد بررسی قرار می‌دهند؛ در حالیکه سیستم‌های تشخیص نفوذ مبتنی بر میزبان[2] (HIDS) [۱۲۹]، رفتارهای میزبان تحت نظارت را ارزیابی می‌نمایند. این سیستم‌ها دارای دید سیستمی بهتر و در نتیجه قدرت بالاتری در کشف نفوذ نسبت به سیستم‌های مبتنی بر شبکه می‌باشند اما به دلیل قرارگیری بر روی میزبان تحت نظارت، نسبت به حملات روت‌کیت‌هایی که ممکن است بر روی میزبان قرار گیرند، آسیب‌پذیر هستند.

ایزوله‌سازی سیستم‌های تشخیص نفوذ مبتنی بر میزبان از میزبان تحت نظارت، یک رویکرد عملی در جهت حفظ این سیستم‌ها در برابر روت‌کیت‌ها به شمار می‌رود و بدین ترتیب می‌توان HIDSها را به عنوان گزینه‌ای مناسب در ایمن‌سازی سیستم‌های کامپیوتری مطرح نمود.

سیستم‌های تشخیص نفوذ مبتنی بر میزبان را می‌توان در لایه‌های متفاوتی از نرم‌افزار سیستم پیاده‌سازی نمود. سیستم‌های سطح کاربر [۱۴۸] به دلیل دارا بودن دیدی محدود نسبت به سیستم، قادر به کشف مناسب پردازه‌های بدرفتار نمی‌باشند و به راحتی می‌توانند از طریق پردازه‌هایی با مجوز بالاتر دور زده شوند. در مقابل سیستم‌های تشخیص نفوذ سطح

[1] Network based Intrusion Detection System (NIDS)
[2] Host based Intrusion Detection System (HIDS)

هسته [۹۹]، علاوه بر داشتن دیدی جامع نسبت به تمامی زیرسیستم‌های هسته، از گزند فرایندهای سطح کاربر نیز در امان هستند. اما همچنان نسبت به حملات روت‌کیت‌های سطح هسته، آسیب‌پذیر می‌باشند.

به طور کلی، تعبیه‌ی HIDSها در لایه‌های هسته یا کاربر، به معنای افزودن یک تابع جدید، به کدی با حجم بالا و بسیار پیچیده می‌باشد که عمل قابل اعتمادی محسوب نمی‌شود. بنابراین ما در این پژوهش به دلایل گوناگون از قبیل وجود روت‌کیت‌های سطح هسته و نیز نیاز به اجازه‌ی دسترسی سطح بالا به حافظه‌ی هسته و ساختار داخلی آن، سیستم تشخیص نفوذ پیشنهادی خود را درون لایه‌ی ناظر تعبیه می‌نماییم. این ناظر از طریق واسط معین و شناخته-شده‌ی x86 ISA با لایه‌های دیگر ارتباط برقرار می‌نماید. استفاده از تکنولوژی مجازی‌سازی پردازنده‌های x86، سیستم تشخیص نفوذ را به وسیله‌ی ایزوله‌سازی کامل آن از سایر لایه‌های نرم‌افزار سیستم، در برابر حملات مقاوم‌تر می‌سازد [۱۱۳].

از سویی دیگر برای اعمال متدهای تشخیص ناهنجاری، نخست نیازمند جمع‌آوری داده‌های مناسب برای تفکیک رفتارهای هنجار و ناهنجار می‌باشیم. به منظور جمع‌آوری داده‌ها، سیستم‌های تشخیص نفوذ می‌توانند از متدهای گوناگونی نظیر پروفایل کردن داده‌ها و یا تحلیل مبتنی بر ویژگی به منظور یافتن دیدی مناسب از فرایندهای در حال اجرا، استفاده نمایند [۱۳۸]. رویدادنگاری فراخوان‌های سیستمی[1] رویکردی است که به منظور ایجاد الگویی مناسب از رفتار فرایندها، از متد تحلیل مبتنی بر ویژگی استفاده می‌کند. تاکنون رویدادنگاری فراخوان‌های سیستمی در لایه‌های گوناگونی از نرم‌افزار سیستم نظیر لایه‌های کاربر، هسته و ناظر، صورت پذیرفته است [۸۶،۴۵،۸۳،۴۷،۱۳۱،۱۱۶،۶۷]. ما در این پژوهش از رویدادنگاری فراخوان‌های سیستمی در لایه‌ی ناظر بهره می‌گیریم تا عملیات جمع‌آوری داده را به صورت امن و به دور از گزند روت‌کیت‌های هسته به انجام رسانیم.

پس از جمع‌آوری امن داده‌ها نخست می‌بایست ویژگی‌های مناسب برای تفکیک رفتار هنجار و ناهنجار را از میان داده‌های ذخیره‌شده استخراج نموده و به فرم یک الگو[2] در بیاوریم و سپس به ساخت یک مدل رفتاری مبتنی بر این الگوها بپردازیم. در این حوزه، سیستم‌های

[1] System call auditing
[2] Pattern

تشخیص نفوذ با دو رویکرد کلی، عملیات ساخت مدل رفتاری را دنبال می‌نمایند. در رویکرد اول که اصطلاحا تشخیص سوء استفاده[۱] نامیده می‌شود، رفتارهای ناهنجار تحت عنوان امضای[۲] بدافزار مدل می‌شوند و یک نفوذ، زمانی کشف می‌شود که با یکی از امضاهای بدافزار، تطبیق داشته باشد. اما رویکرد دوم که اصطلاحا تشخیص ناهنجاری[۳] نامیده می‌شود، به مدل‌سازی رفتارهای هنجار سیستم می‌پردازد و یک نفوذ، زمانی کشف می‌شود که با مدل هنجار تطبیق نداشته باشد.

رویکرد تشخیص سوء استفاده در شناسایی نفوذهای شناخته‌شده بسیار توانمند است و به همین سبب، هم‌اکنون در بسیاری از سیستم‌های تجاری به کار گرفته شده‌است؛ اما بزرگترین نقص آن در عدم توانایی کشف و شناسایی رفتارهای نفوذی جدیدی می‌باشد که امضای آن برای سیستم شناخته‌شده نیست. رویکرد تشخیص ناهنجاری با هدف برطرف‌سازی این نقص عمده‌ی رویکرد اول ارائه شده و به همین سبب در دهه‌های اخیر با استقبال چشمگیری در مجامع علمی روبروست.

این پژوهش در صدد است تا از طریق سیستم‌های ایمنی مصنوعی[۴] به عنوان یکی از شاخه-های هوش محاسباتی، به تشخیص ناهنجاری در سیستم‌های کامپیوتری بپردازد. سیستم‌های ایمنی مصنوعی از سیستم ایمنی انسانی[۵] الهام گرفته‌اند و به دلیل خصوصیاتی نظیر خودسازماندهی، توزیع‌شدگی و سبک بودن، گزینه‌ی مناسبی برای ایجاد سیستم‌های تشخیص ناهنجاری به حساب می‌آیند.

به منظور جمع‌آوری کلیه‌ی خصوصیات ذکرشده در یک چارچوب تشخیص نفوذ، در این پژوهش به ارائه‌ی سیستمی نوین با عنوان SHADuDT می‌پردازیم. این سیستم در حقیقت نوعی معماری امن و مبتنی بر ناظر است که از یک سو با بکارگیری مؤلفه‌ای تحت عنوان رویدادنگار امن (SHADuDT_SA) به جمع‌آوری امن اطلاعات مرتبط با فراخوان‌های سیستمی و آرگومان‌های آن در لایه‌ی ناظر یا مانیتور ماشین مجازی[۶] می‌پردازد و به این ترتیب از گزند

[1] Misuse Detection
[2] Signature
[3] Anomaly Detection
[4] Artificial Immune System (AIS)
[5] Human Immune System (HIS)
[6] Virtual Machine Monitor (VMM)

روت‌کیت‌های هسته در امان می‌ماند و از سویی دیگر از نسل دوم سیستم‌های ایمنی مصنوعی به عنوان متد تشخیص ناهنجاری (SHADuDT_DM) بهره می‌گیرد.

تاکنون بسیاری از سیستم‌های تشخیص نفوذ، عملکرد سیستم ایمنی انطباقی را شبیه‌سازی نموده‌اند اما ایده‌ای جدید در این حوزه که با عنوان تئوری خطر [۹۳،۹۴،۱۴۳] شناخته می‌شود، به منظور ارائه‌ی مدلی دقیق‌تر از فرایندهای زیستی سیستم‌های ایمنی انسانی، علاوه بر سیستم ایمنی انطباقی، عملکرد سیستم ایمنی طبیعی و روابط این دو با یکدیگر را نیز شبیه‌سازی می‌کند.

SHADuDT_DM در میان الگوریتم‌های موجود در حوزه‌ی نسل دوم سیستم‌های ایمنی مصنوعی جای می‌گیرد اما بر خلاف الگوریتم‌های مبتنی بر تئوری خطر پیشین نظیر DCA [۵۰-۵۶] و TLR [۱۲۳-۱۲۵] که به سیگنال‌های خطر خارجی نیازمند هستند، این روش سیگنال‌های مورد نیاز خود را از طریق ساختار داده‌های هنجار و ناهنجار آموزش تولید می‌نماید و برای تولید سیگنال، به منابع خارجی نیازمند نیست. به دلیل استفاده از ساختار داده‌های آموزش، این روش دارای خطای کمتر و کارایی بهتری نسبت به روش‌های تئوری خطر پیشین است و به همین سبب می‌تواند به عنوان یک طبقه‌بند مناسب برای تفکیک رفتارهای هنجار و ناهنجار مورد استفاده قرار گیرد.

به این ترتیب سیستم SHADuDT می‌تواند با بهره‌گیری همزمان از مزایای تکنولوژی ناظر و تئوری خطر، هم از گزند روت‌کیت‌های هسته مصون بماند و هم با متدی دقیق و الهام گرفته از سیستم ایمنی انسانی، به تفکیک رفتارهای هنجار و ناهنجار سیستم بپردازد.

۱-۳ سازمان‌دهی مستند

ادامه‌ی این مستند به صورت زیر سازمان‌دهی می‌شود. فصل دوم به تشریح مفاهیم مرتبط با این پژوهش می‌پردازد. بدافزارها و انواع آن، روت‌کیت‌ها و سیر تکاملی آنها در انجام فعالیت‌های نفوذی، سیستم‌های تشخیص نفوذ و تکنیک‌های رایجی که تاکنون در این حوزه بکار گرفته شده‌اند، سیستم‌های ایمنی انسانی و سیر تکاملی تئوری‌های موجود در این حوزه، سیستم‌های ایمنی مصنوعی و شیوه‌ی الهام‌پذیری آنها از سیستم‌های ایمنی انسانی و در نهایت مجازی-

سازی و خصوصیات ممتاز آن در جهت افزایش امنیت سیستم و پیاده‌سازی سیستم‌های امنیتی، از جمله مطالبی است که در این فصل به آن پرداخته خواهد شد.

فصل سوم به بررسی پژوهش‌های مرتبط با جنبه‌های گوناگون چارچوب پیشنهادی می-پردازد. از آنجا که رویدادنگاری فراخوان‌های سیستمی از طریق مؤلفه‌ی رویدادنگار امن و تشخیص فعالیت‌های ناهنجار به کمک مکانیزم تشخیص ناهنجاری، دو بخش حساس SHADuDT را تشکیل می‌دهند، بنابراین رئوس مطالب این فصل به بررسی رویکردهای گوناگون موجود در حوزه‌ی رویدادنگاری فراخوان‌های سیستمی و مکانیزم‌های متنوعی که تاکنون به منظور تشخیص ناهنجاری مبتنی بر میزبان بکار گرفته شده‌اند، تخصیص می‌یابد.

فصل چهارم به طور کامل به شرح و توصیف چارچوب پیشنهادی و یکایک مؤلفه‌های اساسی آن می‌پردازد و بیان می‌کند که SHADuDT نوعی معماری امن و مبتنی بر ناظر است که از یک سو با بکارگیری مؤلفه‌ای تحت عنوان رویدادنگار امن به جمع‌آوری امن اطلاعات مرتبط با فراخوان‌های سیستمی در لایه‌ی مانیتور ماشین مجازی می‌پردازد و از سویی دیگر از الگوریتمی نوین در حوزه‌ی تئوری خطر، به عنوان متد تشخیص ناهنجاری بهره می‌گیرد.

فصل پنجم به ارزیابی کارایی چارچوب پیشنهادی از جنبه‌های گوناگون می‌پردازد. ارزیابی امنیتی غیررسمی SHADuDT، بررسی قدرت تشخیص این چارچوب در مقابله با انواع نفوذها، مقایسه‌ی قدرت تشخیص روش پیشنهادی با روش‌های کلاسیک موجود در حوزه‌ی سیستم-های ایمنی مصنوعی نظیر الگوریتم‌های انتخاب غیرخودی و نیز الگوریتم‌های تئوری خطر پیشین نظیر DCA و TLR و در نهایت بررسی سربارهای SHADuDT از منظر زمان اجرا و میزان حافظه‌ی مصرفی، رئوس مطالب این فصل را به خود تخصیص می‌دهند.

فصل ششم، به بررسی جزئی‌تر الگوریتم تشخیص نفوذ SHADuDT_DM می‌پردازد. آزمایشات و تحلیل‌های ارائه‌شده در این فصل، الگوریتم SHADuDT_DM را نه به عنوان الگوریتمی ویژه‌ی تشخیص نفوذ، بلکه به عنوان یک طبقه‌بند عام، با قدرت طبقه‌بندهای رایج موجود در حوزه‌ی یادگیری ماشین نظیر بیزین، SVM و kNN مقایسه می‌نمایند.

در نهایت فصل هفتم، کلیه‌ی نتایج حاصل از این پژوهش و راهکارهایی که می‌توانند به عنوان پژوهش‌های آینده مد نظر قرار گیرند را با جزئیات مطرح می‌نماید.