
بسم الله الرحمن الرحیم
الحمد لله رب العالمین الرحمن الرحیم مالک یوم الدین
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

تشخیص ناهنجاری از طریق کنترل جامعیت داده هسته سیستم عامل مبتنی بر رویکرد سیستم ایمنی مصنوعی

استادان راهنما

دکتر رضا عزمی

دکتر محسن افشارچی

دانشجو

سوده بهروزی‌نیا

اسفند ماه سال ۱۳۹۲

کلیه دستاوردهای این تحقیق متعلق به

دانشگاه الزهرا(س) است.

تقدیم

به پاس تعبیر عظیم و انسانی شان از کلمه ایثار و از خودگذشتگی شان

به پاس عاطفه سرشار و گرمای امید بخش وجودشان که در این سردترین روزگاران، بهترین پشتیبان است

به پاس قلب های بزرگ شان که فریادرس است و سرگردانی و ترس در پناهشان به شجاعت می گراید

و

به پاس محبت های بی دریغشان که هرگز فروکش نمی کند

این مجموعه را به پدر و مادر فداکار و خواهر و برادر مهربانم تقدیم می کنم.

قدردانی

سپاس بی کران پروردگار یکتا را که هستی مان بخشید و به طریق علم و دانش رهنمونمان شد و به همنشینی رهروان علم و دانش مفتخرمان نمود و

خوشه چینی از علم و معرفت را روزیمان ساخت.

سپاس خدای را که سخنوران، در ستودن او بمانند و شمارندگان، شمردن نعمت های او ندانند و کوشندگان، حق او را گزاردن نتوانند. و سلام

و درود بر محمّد و خاندان پاک او، طاهران معصوم، هم آنان که وجودمان وامدار وجودشان است.

و با سپاس از پدر و مادری به استواری کوه و مهربانی الهی که مرا الفبای زندگی آموختند و امتنان بیکران از مساعدت های بی شائبه ی استاد

عالیقدرم دکتر رضا عزمی که از محضر پر فیض تدریسشان، بهره ها برده ام.

باشد که بتوانم بخشی از زحمات همگی اتان را سپاس گویم.

چکیده

یکی از چالش‌های مهم در مبحث امنیت سیستم‌های کامپیوتری، تشخیص نفوذ و فعالیت‌های نفوذی به سیستم می‌باشد. در همین راستا، سیستم‌عامل که به عنوان منبع مهم اجرای برنامه‌های کامپیوتری به حساب می‌آید، نقش مهمی در تامین امنیت اطلاعات ایفا می‌کند. سیستم‌های کامپیوتری به علت پیچیدگی و گستردگی، همیشه در معرض حملات و روت‌کیت‌ها قرار دارند. به همین جهت تشخیص نفوذ، هم‌اکنون به یکی از رویکردهای فعال در تحقیقات امنیتی تبدیل شده است. این تحقیقات دارای دو چالش عمده می‌باشند: نخست بستر جمع‌آوری امن اطلاعات و دوم ایجاد روشی دقیق و مبتنی بر رفتار روت‌کیت‌ها برای تشخیص نفوذ.

در این پژوهش، به منظور تشخیص نفوذ و مقابله با حملات و روت‌کیت‌های سطح هسته، سیستم تشخیص نفوذی تحت عنوان *KLrtD*[1] ارائه شده است. این سیستم نوعی معماری امن و مبتنی بر ناظر دارد که از یک سو با بکارگیری ابزار طراحی شده‌ی *KLdG*[2] به جمع‌آوری داده‌های مورد نیاز از سطح هسته می‌پردازد و از سویی دیگر با بهره‌گیری از روشی الهام گرفته از تئوری خطر و خروجی سه ابزار طراحی شده‌ی *KLrtD_IC*[3]، *KLrtD_AD*[4] و *KLrtD_SB*[5] که به ترتیب از روش‌های کنترل جامعیت، تشخیص ناهنجاری و تشخیص مبتنی بر امضا برای تولید سیگنال‌های ورودی استفاده می‌کنند، حملات، روت‌کیت‌ها و ناهنجاری‌های سیستمی را تشخیص می‌دهد.

نتایج حاصل از ارزیابی‌ها، حاکی از این است که سیستم *KLrtD* به علت استفاده از یک روش ترکیبی از تکنیک‌های مختلف و رویکردی مبتنی بر ناظر، به خوبی روت‌کیت‌های سطح هسته را شناسایی کرده و قادر است هم‌ردیف سیستم‌های تشخیص نفوذ مبتنی بر میزبان و در مواقعی، بهتر از آن‌ها، به تشخیص روت‌کیت‌ها و بدافزارهای سطح هسته بپردازد.

کلمات کلیدی: روت‌کیت، کنترل جامعیت، تشخیص ناهنجاری، تشخیص مبتنی بر امضا، سیستم ایمنی مصنوعی، تئوری خطر، تکنولوژی ناظر

---

[1] *Kernel Level rootkit Detection (KLrtD)*
[2] *Kernel Level data Gathering (KLdG)*
[3] *KLrtD_Integrity Checking (KLrtD_IC)*
[4] *KLrtD_Anomaly Detection (KLrtD_AD)*
[5] *KLrtD_Signature Based (KLrtD_SB)*

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

فصل اول : مقدمه و هدف پژوهش

۱-۱-مقدمه

رشد باورنکردنی بدافزارهای کامپیوتری و از طرفی تمایل بیش از پیش کاربران به استفاده از محیط‌های شبکه‌ای و توزیع شده به منظور اشتراک گذاشتن اطلاعات، سبب شده است که اهمیت امنیت در سیستم‌های کامپیوتری خودنمایی بیشتری داشته باشد. با توجه به همین موضوع، یکی از چالش‌های اساسی در این حوزه، بحث امنیت و تشخیص فعالیت‌های خرابکارانه و هرگونه نفوذ به آن‌ها می‌باشد که جامعیت[۱]، محرمانگی[۲] و یا دسترسی[۳] به یک منبع را در یک سیستم کامپیوتری به خطر می‌اندازد. با توجه به تلاش‌های فراوان برای مقابله با فعالیت‌های خرابکارانه، امروزه دیگر صحبت از طراحی یک سیستم اطلاعاتی بدون درنظر گرفتن جوانب امنیتی آن امری منسوخ است.

حملات و نفوذ به سیستم‌های کامپیوتری از طریق بدافزارها[۴] انجام می‌شوند. بدافزارها، یکی از ابزارها و اقدامات ضد امنیتی هستند و به برنامه‌هایی اطلاق می‌شوند که بدون اجازه صاحب سیستم، قصد انجام کارهای ناخواسته یا خرابکارانه را در سیستم دارند. ویروس‌ها، کرم‌واره‌ها، اسب‌های تراوا[۵]، شماره‌گیرها[۶]، درهای پشتی[۷]، نرم‌افزارهای جاسوسی[۸] و روت‌کیت‌ها[۹] نمونه‌ای از انواع بدافزارهای موجود در دنیای امنیت می‌باشند. به دلیل طبیعت تغییرپذیر، روبه‌رشد و گسترده این مقوله، مقابله با آن‌ها یکی از مسائل چالش‌برانگیز و ضروری در امنیت سیستم‌های کامپیوتری محسوب می‌شود.

روت‌کیت‌ها بدافزارهایی هستند که اغلب، آن‌ها را به خودی خود نمی‌توان مخرب یا خطرناک دانست، بلکه قرارگرفتن آن‌ها در کنار ویروس‌ها یا کرم‌واره‌های اینترنتی یا نوع

---

[1] *Integrity*
[2] *Confidentiality*
[3] *Availability*
[4] *Malware*
[5] *Trojan Horse*
[6] *Dialer*
[7] *Backdoor*
[8] *Spyware*
[9] *Rootkit*

استفاده از آن‌ها است که به آنان ماهیتی خطرناک می‌بخشد. شناسایی روت‌کیت بسیار مشکل‌تر از بدافزارهای دیگر است زیرا روت‌کیت‌ها جایگزین برنامه‌های اجرایی مهم سیستم‌عامل شده و در گاهی مواقع جایگزین خود هسته می‌شوند و به دیگر بدافزارها این اجازه را می‌دهند که از طریق درب‌پشتی و پنهان‌شدن در سیستم‌عامل به آن نفوذ کنند. با توجه به همین مشکلات و همین‌طور قدرت غیرقابل انکار روت‌کیت‌ها در حمله و نفوذ به سیستم، تشخیص و مقابله با آن‌ها یکی از مباحث مهم امنیتی به‌شمار می‌رود.

در همین راستا، هدف اصلی این پژوهش ارائه‌ی یک سیستم تشخیص نفوذ مبتنی بر میزان است که تا حدی با بهبود کارهای پیشین، گامی در جهت رسیدن به یک سیستم امن در شناسایی بدافزارهای پنهان سطح هسته بردارد. در ادامه، رویکردهای کلیدی این پژوهش در بخش ۱-۲ و شیوه‌ی سازماندهی مستند در بخش ۱-۳ بررسی می‌شود. 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 سیستم تشخیص نفوذ مبتنی بر میزبان می‌باشد. ارائه و پیاده‌سازی یک سیستم جدید در حوزه‌ی تشخیص نفوذ، نیازمند بررسی دقیق مسائل گوناگونی نظیر مکان پیاده‌سازی، داده‌های موردنیاز، تحلیل روت‌کیت‌ها، نحوه‌ی تولید امضاها، جمع‌آوری امضاهای موجود و نیز استفاده از روش تشخیصی مناسب می‌باشد.

سیستم‌های تشخیص نفوذ، بر اساس موقعیت قرارگیری و دریافت منبع اطلاعاتی، به دو دسته‌ی مبتنی بر شبکه و مبتنی بر میزبان تقسیم می‌شوند. سیستم‌های مبتنی بر شبکه[1] *(NIDS)* [۳]، از بسته‌ها و ترافیک شبکه به عنوان منبع اصلی اطلاعات برای تصمیم‌گیری پیرامون نفوذ استفاده می‌کنند. سیستم‌های مبتنی بر میزبان[2] *(HIDS)* [۴] که در این پژوهش مدنظر قرار گرفته شده‌اند، با بررسی و ارزیابی رفتارهای میزبان، دید سیستمی و قدرت بالایی در تشخیص نفوذ دارند.

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

سیستم‌های تشخیص مبتنی بر میزبان را از لحاظ مکان پیاده‌سازی می‌توان به سه سطح کاربری، هسته سیستم‌عامل و سیستم ناظر طبقه‌بندی کرد. این سیستم‌ها در سطح کاربر مانند یک نرم‌افزار کاربردی می‌توانند پردازه‌های در حال اجرا و رفتار آن‌ها را کنترل کنند، اما نمی‌توانند از خود محافظت کرده و دید جامعی به اطلاعات درون هسته داشته باشند [۶،۵]. دسته‌ی دیگری از این روش‌ها مانند [۷] در سطح هسته سیستم‌عامل و با ایجاد تغییرات در کد هسته بر عملیات حساس نظارت دارند. این دسته عموما به بررسی داده‌های ایستا و تنها نحوه‌ی دسترسی به داده‌های حساس می‌پردازند و از دید روت‌کیت‌ها کاملا محافظت نمی‌شوند [۹،۸]. گفتنی است برخی از راه‌حل‌های محدود نرم‌افزار مانند [۱۰] که برای حفاظت از زیر بخش‌های هسته معرفی شده‌اند، در حال حاضر هیچ‌کدام اثبات کامل و مطمئنی نسبت به امنیت روش خود ارائه نکرده‌اند.

با توسعه‌ی فناوری ماشین مجازی که در بسیاری از محیط‌ها مورد استفاده قرار گرفته شده است، نظارت بر رویدادهای سطح هسته و حافظت از داده‌ها نیز بر بستر این فناوری و در ناظر توسعه یافته است، به طوری که می‌توان ادعا کرد یکی از عوامل پیشرفت این فناوری امکان نظارت بیرونی بر ماشین مجازی *(VMI)* بوده است [۱۴،۱۳،۱۲،۱۱،۲]. استفاده از این فناوری توسط [۱۱] و با بکارگیری *VMI* در شناسایی بدافزارها مورد توجه بیشتری قرار گرفته است. پس از آن *Lares*[۵]، *SIM* [۱۰]، *TraDic* [۲]، *Wizard* [۹]، *HyperSafe* [۱۲] و *HyperCheck* [۱۳] برای کنترل جامعیت هسته در ناظر قرار گرفته و از فناوری مجازی‌سازی بهره بردند.

بنابراین این پژوهش به دلایل گوناگون از قبیل وجود روت‌کیت‌های سطح هسته و نیز نیاز به اجازه‌ی دسترسی سطح بالا به هسته و ساختار داخلی آن، سیستم تشخیص نفوذ پیشنهادی را درون لایه‌ی ناظر تعبیه نموده است. استفاده از تکنولوژی مجازی‌سازی، سیستم تشخیص نفوذ را به‌وسیله‌ی ایزوله‌سازی کامل آن از سایر لایه‌های نرم‌افزار سیستم، در برابر حملات مقاوم‌تر می‌سازد [۱۴].

این سیستم پیشنهادی برای اعمال روش‌های تشخیص، نیازمند جمع‌آوری داده‌های مناسبی برای تشخیص و تفکیک رفتار هنجار یا ناهنجار سیستم میزبان می‌باشد. برای بررسی همه‌جانبه و جامع از هسته‌ی سیستم‌عامل میزبان و پردازه‌های درحال اجرا، بایستی اطلاعات

کاملی نظیر ساختارداده‌های حیاتی شامل داده‌های کنترلی و غیرکنترلی، ثبات‌ها، دنباله فراخوانی‌های سیستمی و همین‌طور اطلاعات پردازه‌های در حال اجرا را از سراسر هسته‌ی سیستم جمع‌آوری کرد. تاکنون جمع‌آوری داده‌ها در محیط‌های گوناگون نظیر محیط بیرونی، محیط داخل میزبان و محیط ناظر صورت پذیرفته است [۱۸،۱۷،۱۶،۱۵]. این پژوهش جمع‌آوری داده‌ها را در لایه‌ی ناظر انجام داده است تا عملیات را به صورت امن و به‌دور از گزند روت‌کیت‌های سطح هسته به انجام برساند.

به طور کلی، سیستم‌های تشخیص نفوذ با دو رویکرد کلی، عملیات تشخیص را دنبال می‌نمایند. در رویکرد اول که اصطلاحا تشخیص مبتنی بر امضا[۱] نامیده می‌شود، رفتارهای ناهنجار تحت عنوان امضای بدافزار مدل می‌شوند و یک نفوذ، زمانی کشف می‌شود که با یکی از امضاهای بدافزار، تطبیق داشته باشد. این سیستم‌ها به جای استفاده از امضاهای بدافزار می‌توانند از امضاهای امن استفاده کنند. در این حالت سیستم زمانی در حالت امن تشخیص داده می‌شود که با امضاهای امن تطبیق داشته باشد. اما رویکرد دوم که اصطلاحا تشخیص ناهنجاری[۲] نامیده می‌شود، به مدل‌سازی رفتارهای هنجار سیستم می‌پردازد و یک نفوذ، زمانی کشف می‌شود که با مدل هنجار تطبیق نداشته باشد.

رویکرد تشخیص مبتنی بر امضا در شناسایی نفوذهای شناخته‌شده بسیار قدرتمند است و به همین سبب، هم‌اکنون در بسیاری از سیستم‌های تجاری به‌کار گرفته شده است؛ اما نقص آن در عدم توانایی کشف و شناسایی رفتارهای نفوذی جدیدی می‌باشد که امضای آن‌ها برای سیستم شناخته شده نیست. رویکرد تشخیص ناهنجاری با هدف برطرف‌سازی این نقص و تشخیص نفوذهای ناشناخته ارائه شده است. با توجه به همین موضوع، سیستم ارائه شده از تلفیق دو روش برای تشخیص نفوذ در سیستم استفاده می‌کند تا همزمان بتواند از مزایای هر دو استفاده نموده و کاستی‌های هر یک را تحت پوشش قرار دهد.

این پژوهش درصدد است تا سیستم پیشنهادی خود را مبتنی بر سیستم‌های ایمنی مصنوعی[۳] ارائه دهد. سیستم‌های ایمنی مصنوعی به دلیل شباهت زیاد با سیستم ایمنی انسانی

---

[1] *Signature based Detection*

[2] *Anomaly Detection*

[3] *Artifial Immune System (AIS)*

و شبیه‌سازی مکانیزم دفاعی بدن، گزینه‌ی مناسبی برای سیستم‌های تشخیص به‌حساب می‌آیند.

به منظور جمع‌آوری کلیه‌ی داده‌های مورد نیاز برای سیستم تشخیص، در این پژوهش ابزاری تحت عنوان *KLdG* طراحی شده است که با نوعی معماری امن و مبتنی بر ناظر به جمع‌آوری امن اطلاعات در لایه‌ی ناظر یا مانیتور ماشین مجازی[1] می‌پردازد. در ادامه سیستمی نوین تحت عنوان *KLrtD* مبتنی بر تئوری خطر [۱۹،۲۰] در سیستم ایمنی ارائه می‌شود که با سه مولفه‌ی مختلف با عناوین *KLrtD_IC*، *KLrtD_AD* و *KLrtD_SB* به جمع‌آوری سیگنال‌های لازم در تشخیص نفوذ می‌پردازد.

سیستم *KLrtD* برای تولید سیگنال امن[2] از روش تشخیص مبتنی بر امضای لیست سفید[3] برای کنترل جامعیت هسته‌ی سیستم‌عامل در مولفه *KLrtD_IC* استفاده می‌کند. این سیستم از سویی دیگر برای تولید سیگنال خطر[4] و *PAMP* به ترتیب از روش‌های تشخیص ناهنجاری و تشخیص مبتنی بر امضای لیست سیاه[5] در مولفه‌های *KLrtD_AD* و *KLrtD_SB* استفاده می‌نماید.

سیستم *KLrtD* همان‌طور که بیان شد، سیگنال‌های مورد نیاز خود را از طریق مولفه‌های مختلف طراحی‌شده، تولید می‌کند. این سیستم به‌دلیل استفاده از داده‌های آموزش جامع و همچنین ترکیبی مناسب از انواع روش‌های تشخیص، کارایی خوبی در میان سیستم‌های تشخیص نفوذ مبتنی بر میزبان در تشخیص روت‌کیت‌های سطح هسته دارد.

به این ترتیب سیستم *KLrtD* می‌تواند با بهره‌گیری همزمان از مزایای تکنولوژی ناظر و تئوری خطر، از گزند روت‌کیت‌های سطح هسته مصون بماند و با روشی دقیق و الهام گرفته از سیستم ایمنی انسانی، به تفکیک رفتار هنجار و ناهنجار سیستم بپردازد.

---

[1] *Virtual Machine Monitor*
[2] *Safe*
[3] *White list*
[4] *Danger*
[5] *Black list*