روش‌های تشخیص بدافزار و توسعه شیوه‌ای جدید در تشخیص بدافزار

محمود کرمی پور

استاد راهنما: دکتر شهریار محمدی

پایان‌نامه برای دریافت مدرک کارشناسی ارشد

مهندسی فناوری اطلاعات-تجارت الکترونیک

شهریور ۱۳۹۲

روش‌های تشخیص بدافزار و توسعه شیوه‌ای جدید در تشخیص بدافزار

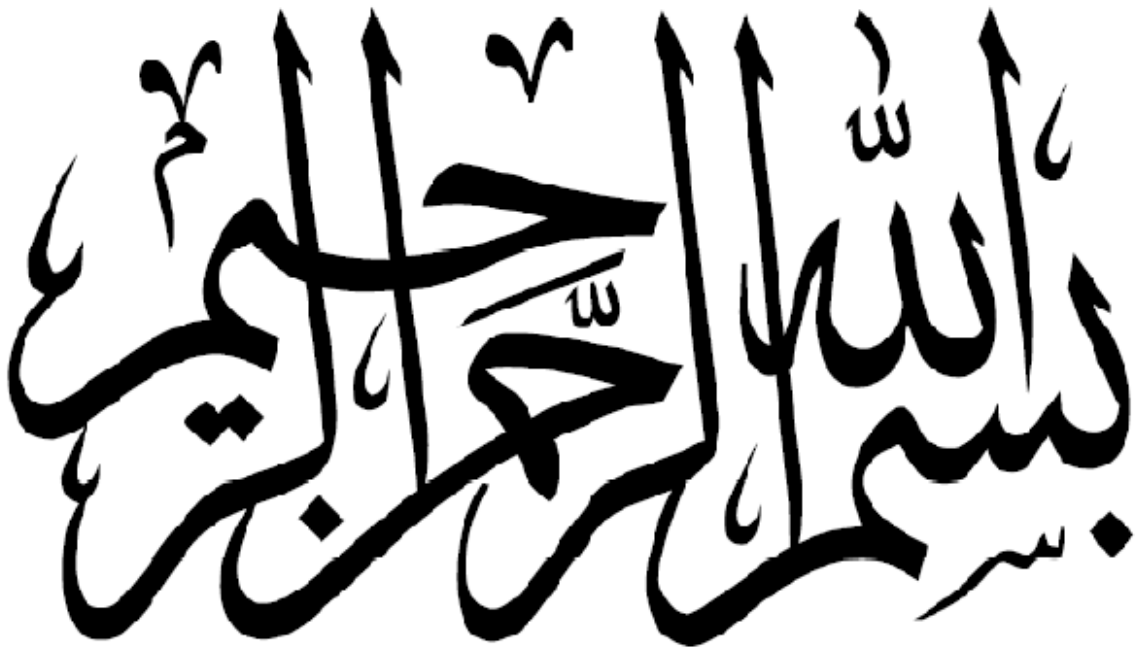
محمود کرمی پور

استاد راهنما: دکتر شهریار محمدی

پایان‌نامه برای دریافت مدرک کارشناسی ارشد

مهندسی فناوری اطلاعات-تجارت الکترونیک

شهریور ۱۳۹۲


بسم الله الرحمن الرحيم

تقدیم به پدر و مادرم

که از نگاهشان صلابت

از رفتارشان محبت

و از صبرشان ایستادگی را آموختم

تاسیس ۱۳۰۷ دانشگاه صنعتي خواجه نصيرالدين طوسي	**بسمه تعالی** **تأییدیه هیأت داوران**	**شماره:** **تاریخ:**

هیأت داوران پس از مطالعه پایان‌نامه و شرکت در جلسه دفاع از پایان‌نامه تهیه شده تحت عنوان :

روش‌های تشخیص بدافزار و توسعه شیوه‌ای جدید در تشخیص بدافزار

توسط آقای **محمود کرمی‌پور** ، صحت و کفایت تحقیق انجام شده را برای اخذ درجه کارشناسی ارشد **رشته مهندسی فناوری اطلاعات گرایش تجارت الکترونیک** در تاریخ **۱۳۹۲/۰۶/ ۲۶** مورد تأیید قرار می‌هند.

۱- استاد راهنمای اول	جناب آقای دکتر **شهریار محمدی**	امضاء
۲- ممتحن داخلی	سرکار خانم دکتر **سمیه علیزاده**	امضاء
۳- ممتحن خارجی	جناب آقای دکتر **داود کریم زادگان مقدم**	امضاء
۴- معاونت آموزشی و تحصیلات تکمیلی دانشکده	جناب دکتر **عماد روغنیان**	امضاء

تاسیس ۱۳۰۷ دانشگاه صنعتی خواجه نصیرالدین طوسی	**بسمه تعالی** **اظهارنامه دانشجو**	**شماره:** **تاریخ:**

اینجانب محمود کرمی پور دانشجوی کارشناسی‌ارشد رشته مهندسی فناوری اطلاعات گرایش تجارت الکترونیک دانشکده مهندسی صنایع دانشگاه صنعتی خواجه نصیرالدین طوسی گواهی می‌نمایم که تحقیقات ارائه شده در پایان‌نامه با عنوان

روش‌های تشخیص بدافزار و توسعه شیوه‌ای جدید در تشخیص بدافزار

با راهنمایی استاد محترم جناب آقای **دکتر شهریار محمدی**، توسط شخص اینجانب انجام شده و صحت واصالت مطالب نگارش شده در این پایان‌نامه مورد تأیید می‌باشد، و در مورد استفاده از کار دیگر محققان به مرجع مورد استفاده اشاره شده است. بعلاوه گواهی می‌نمایم که مطالب مندرج در پایان نامه تا کنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب یا فرد دیگری در هیچ جا ارائه نشده است و در تدوین متن پایان‌نامه چارچوب (فرمت) مصوب دانشگاه را بطور کامل رعایت کرده‌ام.

امضاء دانشجو:

تاریخ:

تاسیس ۱۳۰۷ دانشگاه صنعتی خواجه نصیرالدین طوسی	**بسمه تعالی** **حق طبع و نشر و مالکیت نتایج**	**شماره:** **تاریخ:**

تقدیر و تشکر

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.

از استاد محترم جناب آقای دکتر شهریار محمدی برای حمایت های بی دریغ ایشان کمال تشکر و قدردانی را دارم.

چکیده

بدافزارها و تهدیدات آنها یکی از بزرگترین چالش‌ها در امنیت و یکپارچگی اطلاعات و شبکه‌های کامپیوتری است. دو روش عمده در تشخیص بدافزار وجود دارد؛ روش مبتنی بر امضا و روش مبتنی بر ناهنجاری. نرم افزارهای آنتی ویروس کنونی از روش‌های مبتنی بر امضا استفاده می‌نمایند. روش‌های مبتنی امضا دقیق هستند اما توانایی تشخیص حملات روز نخست و ناشناخته را ندارند. ما می‌توانیم با استفاده از روش‌های مبتنی بر ناهنجاری و تطبیق آنها با روش‌های یادگیری نظارتی توانایی تشخیص بدافزارهای جدید را افزایش دهیم. دو نوع خصیصه وجود دارد که یادگیری نظارتی در تشخیص بدافزار از آن‌ها استفاده می‌کند؛ خصیصه‌های ایستا و خصیصه‌های پویا. خصیصه‌های ایستا از ساختار فایل اجرایی دودویی و خصیصه‌های پویا با اجرای فایل در محیط واقعی یا شبیه‌سازی شده به‌دست می‌آیند. در این تحقیق روشی مبتنی بر یادگیری ماشین بر مبنای خصیصه‌های ترکیبی ایستا-پویا ارائه گردیده است. تعداد فراوانی از بدافزارهای جدید هر روزه بر روی اینترنت پخش می‌شوند و روشی جهت تشخیص این نمونه‌های جدید و مقاصد آنها نیاز است. تحلیل این بدافزارها توسط عامل انسانی زمان‌بر و پرخطاست و توسعه روش‌های خودکار جهت تحلیل حجم بالای نمونه الزامی است. روش ترکیبی پیشنهادی توانایی تحلیل حجم بالای نمونه اجرایی و تشخیص بدافزارهای ناشناخته را دارد و نیز با توجه به استفاده از خصیصه‌های ایستا و پویا در کنارهم از درصد هشدار اشتباه پایینی برخوردار است. استفاده از خصیصه-های ایستا و پویا در کنار یکدیگر سبب افزایش درصد تشخیص و دقت تشخیص نسبت به استفاده جداگانه از آن‌ها می‌شود.

کلمات کلیدی: تشخیص بدافزار، روش ترکیبی، روش ایستا-پویا، یادگیری ماشین، دسته‌بندی

فهرست مطالب

فهرست جدول‌ها

فهرست شکل‌ها

فصل ۱

کلیات موضوع

۱-۱ مقدمه

اینترنت به‌عنوان بخش اساسی از زندگی روزانه مردم تبدیل شده است زیرا که خدمات مختلف اکنون توسط این شبکه ارتباطی عرضه می‌شوند. اینترنت از یک شبکه ارتباطی به شبکه‌ای از منابع ارائه‌دهنده اطلاعات، شکل جدیدی از تعاملات اجتماعی و بازاری برای فروش محصولات و ارائه سرویس‌ها و خدمات متنوع تبدیل گردیده است. بانکداری اینترنتی و تبلیغات از جمله کاربردهای تجاری اینترنت هستند. گسترش فناوری اطلاعات و تجارت الکترونیک از یک سو فرصت‌های جدید برای محیط‌های کسب‌وکار فراهم نموده است؛ از دیگر سو مسائلی همانند امنیت و محرمانگی اطلاعات در دنیای مجازی و استفاده از اینترنت به‌عنوان ابزاری جهت گسترش انواع بدافزار و پیدایش شیوه‌های جدید کلاه‌برداری مشکلاتی هستند که در دنیای جدید مجازی بروز پیداکرده‌اند. همانند دنیای واقعی در دنیای مجازی نیز افرادی هستند که تمایلات مجرمانه و شوم دارند. بدافزارها (نرم‌افزارهایی که اهداف بد دارند) به این افراد کمک می‌نمایند که به مقاصد مجرمانه خود برسند. شناسایی بدافزارها نخستین مرحله در پیشگیری سیستم‌های کامپیوتری در مواجه با از دست دادن بالقوه اطلاعات و به خطر افتادن آن‌هاست. راه‌های مختلفی برای شناسایی بدافزارها وجود دارد. یک شناساگر بدافزار تلاش می‌کند عملکردها و برنامه‌های نادرست را بیابد. شناسایی بدافزارها مهم‌ترین مرحله در پیشگیری سیستم‌های کامپیوتری در مقابل آلوده شدن، محافظت در برابر از دست دادن اطلاعات و به خطر افتادن آن‌هاست. روش‌های بسیاری برای شناسایی بدافزارها وجود دارد تا از اجرای آن‌ها جلوگیری شود.

اصلی‌ترین روش‌ها برای شناسایی بدافزارها بر اساس ناهنجاری[1]، امضا[2]، ویژگی‌ها[3] است. این روش‌ها محدود به شناسایی بدافزارها نمی‌شوند، بلکه برای شناسایی نفوذ در شبکه‌های کامپیوتری و دیگر زمینه‌ها نیز کاربرد دارند.

بیشتر نرم‌افزارهای آنتی‌ویروس، با استفاده از تکنیک امضا ویروسی عمل می‌کنند که در نتیجه آن به طور پیوسته با مجموعه‌ای از امضاها روبرو هستند. این روش یک روش انفعالی است، به‌محض آنکه یک امضا برای یک اکسپلویت[4] ایجاد می‌شود، این اکسپلویت توسط نرم‌افزارهای آنتی‌ویروس به‌راحتی شناسایی خواهد شد.

روش‌هایی که بر اساس ناهنجاری به وجود آمده در سیستم طراحی می‌شوند بر اساس الگوهایی در داده‌ها شناسایی می‌شود که متفاوت از رفتار مورد انتظار است. ناهنجاری‌ها در داده‌ها می‌تواند متناسب با تغییرات مهم در سیستم باشد. اگر یک کامپیوتر با الگوی ترافیکی اینترنتی ناهنجار مواجه شود این امر نشان می‌دهد که مورد حمله واقع‌شده و اطلاعات در حال فاش شدن است (چاندولا و همکاران[5]، ۲۰۰۹).

روند شناسایی یک سیستم بدافزار نشان می‌دهد که چگونه اطلاعات در مورد برنامه جمع‌آوری شده است و روش شناسایی نشان می‌دهد که چگونه این اطلاعات مورد استفاده قرار می‌گیرند. رویکردهای اصلی برای تحلیل و آنالیز بدافزارها شامل آنالیز ایستا، آنالیز پویا و ترکیبی از این دو است.

آنالیز ایستا از اطلاعات ساختاری و ترکیبی از یک برنامه استفاده می‌کند تا ناهنجاری‌های آن را مشخص کند. قبل از اینکه یک برنامه اجرا شود، اطلاعات ایستا قابل‌اجرا شناسایی می‌شوند مثل داده‌های سرآیند[6] و بیت‌های پشت سرهم. این کار به این منظور انجام می‌شود که اگر ناهنجاری وجود دارد مشخص شود. آنالیز ایستا قادر است همه مسیرهای موجود در یک برنامه که ممکن است در زمان اجرا قرار گیرد را آنالیز کند، بااین‌وجود معمولاً دربرگیرنده همه حالات ممکن برنامه نمی‌شود چون داده‌های

[1] Anomaly-based
[2] Signature-based
[3] Specification-based
[4] Exploit
[5] Chandola
[6] Header data