به نام خدا

دانشگاه صنعتی امیرکبیر
(پلی‌تکنیک تهران)
دانشکده کامپیوتر و فن آوری اطلاعات

پایان نامه جهت دریافت درجه کارشناسی ارشد

در رشته مهندسی کامپیوتر گرایش معماری کامپیوتر

کشف تعاملی کرم با استفاده از شبکه‌های نظیر به نظیر

Collaborative Worm Detection using Peer-to-Peer Systems

نگارش
جواد طاهری

استاد راهنما
دکتر محمدکاظم اکبری

تیر ۱۳۸۷

بسمه تعالی

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

فرم اطلاعات پایان‌نامه
کارشناسی- ارشد و دکترا
کتابخانه مرکزی

شماره مدرک:

مشخصات دانشجو	نام خانوادگی : طاهری	نام: جواد	شماره دانشجویی: ۸۴۱۳۱۰۲۳
	دانشکده: مهندسی کامپیوتر و فن‌آوری اطلاعات	رشته: مهندسی کامپیوتر	گروه: معماری کامپیوتر
عنوان	کشف تعاملی کرم با استفاده از شبکه‌های نظیر به نظیر		
Title	Collaborative Worm Detection using Peer-to-Peer Systems		

استاد راهنما	نام خانوادگی: اکبری فتیدهی	درجه و رتبه	استاد راهنما	نام خانوادگی:	درجه و رتبه
	نام: محمد کاظم	دانشیار		نام:	
استاد مشاور	نام خانوادگی:	درجه و رتبه	استاد مشاور	نام خانوادگی:	درجه و رتبه
	نام:			نام:	

دانشنامه	کارشناسی ○ ارشد ⊙ دکترا ○	سال تحصیلی: ۸۷-۸۶
نوع پروژه	کاربردی ⊙ نظری ○ توسعه ای ⊙ بنیادی ○	
مشخصات ظاهری	تعداد صفحات ۱۱۵	تصویر ⊙ جدول ⊙ نمودار ○ نقشه ○ واژه‌نامه ○ تعداد مراجع ۸۰ ضمائم ○ تعداد صفحات:
زبان متن	فارسی ⊙ انگلیسی ○	چکیده: فارسی ⊙ انگلیسی ⊙
یاداشت		
توصیفگر		
کلید واژه فارسی	کرم، بازداری کرم، شبکه‌های نظیربه‌نظیر، بازداری تعاملی کرم	
Key word of English	Worms, Worm Containment, Peer-to-Peer Systems, Collaborative Worm Containment.	

این مجموعه را تقدیم می‌کنم به پدر بزرگوار

و مادر مهربانم

که تمام آنچه که دارم را مدیون ایشان می‌دانم.

توانا بود هر که دانا بود...

قدردانی

از استاد بزرگوارم، جناب آقای دکتر محمدکاظم اکبری که در سایه رهنمودها و نظرات ایشان این پایان‌نامه تهیه و تکمیل گردید، نهایت تشکر و قدردانی را دارم.

همچنین از دوستان عزیزم، آقایان حامد جانزاده، بهنام قوامی و مجید یوسفی، و هم‌آزمایشگاهی‌های گرانقدر در آزمایشگاه تحقیقاتی سیستم‌های موازی که در مدت زمان انجام این پروژه و تدوین رساله، کانون دوستانه و پرمهری را برای من ایجاد کردند، قدردانی می‌کنم.

از مرکز تحقیقات مخابرات ایران نیز به دلیل پشتیبانی مالی و همکاری‌های به عمل آمده در راستای انجام این پایان‌نامه صمیمانه قدردانی می‌شود.

این پایان‌نامه با ارجاع به نامه ۵۰۰/۱۵۳۷۰/ت مورخ ۸۵/۱۲/۱۳، تحت حمایت مالی مرکز تحقیقات مخابرات ایران قرار گرفته است.

فهرست مطالب

فهرست شکل‌ها

فهرست جدول‌ها

چکیده

کرم‌ها- برنامه‌هایی که به صورت اتوماتیک در شبکه‌های کامپیوتری منتشر می‌شوند- یک خطر جدی برای کامپیوترهای متصل به اینترنت به شمار می‌آیند. این برنامه‌ها، با به کارگیری آسیب‌پذیری‌های موجود در برنامه‌ها و نرم‌افزارها، کامپیوترهای هدف را آلوده ساخته و از این ماشین‌ها برای اجرای مقاصد مغرضانه خود استفاده می‌کنند. تجارب گذشته نشان می‌دهد که سرعت انتشار کرم‌ها می‌تواند بسیار سریعتر از آن باشد که بتوان با دخالت مستقیم انسان آن‌ها را متوقف نمود. به همین دلیل، لازم است تا مکانیزم بازدارکننده[1] انتشار کرم‌ها، مکانیزمی کاملا خودکار باشد.

در این پایان‌نامه، با بررسی مکانیزم Wormshield که یکی از جدیدترین مکانیزم‌های ارائه شده برای تشخیص و جلوگیری از انتشار کرم‌ها است، به بررسی برخی از مشکلات آن پرداخته و سپس دو پیشنهاد برای بهبود این مشکلات ارائه می‌کنیم. یکی از این مشکلات، ضعف در تشخیص شناسایی کرم‌های زیردامنه‌ای است. برای حل این مشکل، ناظرها را که در سیستم قبلی در یک شبکه Chord قرار دارند، در یک سیستم نظیر به نظیر جدید به نام TAC سازماندهی می‌کنیم. در اینصورت ناظرهای هر زیردامنه که با یکدیگر یک دامنه آدرس بزرگتر را تشکیل می‌دهند، نسبت به وجود یکدیگر آگاه خواهند بود و اشتراک اطلاعات ترافیک به نحو مناسب‌تری انجام می‌گیرد. در نتیجه

[1] Containment

کرم‌های زیردامنه‌ای سریعتر کشف می‌گردند. یکی دیگر از مسائل مطرح در این سیستم، نیاز به توان محاسباتی بالا و نیز ترافیک قابل ملاحظه در مخابرات میان ناظرها(به دلیل حجم بالای ترافیک) است. برای بهبود این مشکل، یک روش جدید و جایگزین برای کشف امضاهای مشکوک ارائه کرده‌ایم. در روش ارائه شده، به جای آنکه امضاهای کرم‌ها با استفاده خاصیت تکرار نمونه‌های کرم و فراتر رفتن تعداد نمونه‌های مشاهده شده از آستانه‌های از پیش تعیین شده تولید گردد، از تاریخچه کرم‌ها به عنوان سندی بر مشکوک و یا عادی بودن آنها استفاده شده است. به این ترتیب علاوه بر اینکه نیاز به شمردن و نگه‌داری امضاهای مختلف کرم‌ها توسط ناظرها مرتفع می‌شود، سرعت کشف و بازداری کرم‌ها نیز به صورت چشمگیری افزایش می‌یابد.

یافته‌های ما نشان می‌دهد که با به کارگیری تکنیک‌های پیشنهاده شده، سرعت کشف امضای کرم Code-RedII که یک نمونه از کرم‌های معروف و مهم است، تا ۱۸٪ افزایش می‌یابد. در مورد به کار بردن شبکه TAC نیز آزمایشات انجام شده از بهبود ۸٪ در مدت زمان تشخیص امضای کرم حکایت می‌کنند.

۱ مقدمه‌ای بر کرم‌های اینترنتی و دسته‌بندی آنها

در این قسمت قبل از تعریف کرم‌ها و نحوه کار آنان، ابتدا به صورت مختصر چند مفهوم امنیتی را در مورد کامپیوتر و شبکه کامپیوتری مورد مطالعه قرار می‌دهیم. با مطالعه این مفاهیم قادر خواهیم بود ضمن داشتن درک بهتری از ساختمان کلی یک کرم کامپیوتری و فلسفه کار آن، تشابهات و تفاوت‌های آن با دیگر موضوعات مطرح را بهتر درک کنیم.

واژه امنیت معمولا در مورد یک سیستم به کار می‌رود. به طور کلی منظور از امنیت یک سیستم، اطمینان از عدم آسیب‌رسانی آن سیستم به منافع و دارایی‌های استفاده کننده در هنگام استفاده از آن اطلاق می‌شود. به عنوان مثال اگر بخواهیم یک دستگاه اتومبیل را در نظر بگیریم، توقع کاربر آن از امنیت دستگاه، بی‌خطر بودن رانندگی با آن و اعتمادپذیری قطعات یدکی اتومبیل می‌باشد. اگر سیستم مورد نظر یک گاوصندوق باشد، منظور از امنیت آن، مقاوم بودن در برابر سرقت اموال و دارایی‌های موجود در آن است و بالاخره اگر سیستم پست را در نظر بگیریم، شخصی که از آن استفاده می‌کند، در صورتی آن را امن تلقی می‌کند که علاوه بر رساندن به موقع نامه به گیرنده، محتویات آن نیز از دید دیگران محفوظ باقی بماند و تغییری در آن ایجاد نگردد. در سه مثال ذکر شده، منافعی که در معرض خطر قرار دارند، به ترتیب جان، دارایی و محرمانگی اطلاعات کاربر می‌باشند.

به عنوان یک سیستم بزرگ و گسترده‌تر، کامپیوترها و شبکه‌های کامپیوتری نیز از این قاعده مستثنی نیستند. اتصال میلیون‌ها دستگاه کامپیوتر در نقاط جغرافیایی گوناگون به یکدیگر، ناشناس ماندن هویت کاربران و نیز ظهور کاربردهای حساسی نظیر تجارت الکترونیکی و تراکنش‌های عظیم مالی، به همراه بسیاری از عوامل دیگر، باعث شده است که امنیت کامپیوتری بیش از پیش مورد توجه قرار گیرد. یکی از مشکلات اساسی که در این زمینه وجود دارد، عدم در نظر گرفتن مفاهیم امنیتی به صورت اساسی در ساختار شبکه اینترنت، در زمان پیدایش آن بوده است[۱]

۱-۱ ارکان امنیت کامپیوتری

امنیت کامپیوتری بر سه رکن اصلی محرمانگی[1]، یکپارچگی[2] و دسترس‌پذیری[3] استوار است. به عبارت دیگر یک سیستم کامپیوتری در صورتی امن خواهد بود که این سه ویژگی را در مورد منابع و اطلاعاتی که با آنها در ارتباط است حفظ نماید. در ادامه این قسمت، این سه مفهوم و مکانیزم‌های مربوط به آنها را به صورت اجمالی مورد مطالعه قرار می‌دهیم[2].

۱-۱-۱ محرمانگی

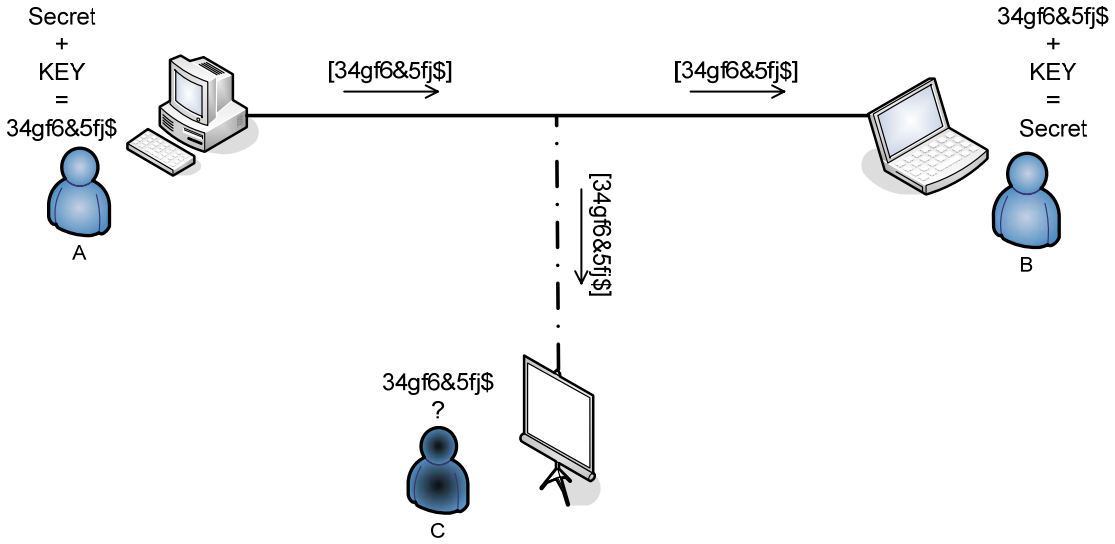
منظور از محرمانگی، اختفای اطلاعات و یا منابع است. نیاز به مخفی نگه داشتن اطلاعات هنگامی احساس می‌شود که از کامپیوترها در مقاطعی همچون امور دولتی و یا نظامی استفاده شود. به عنوان مثال، سازمان‌ها و موسسات دولتی یا نظامی معمولا امکان دسترسی به اطلاعات خود را تنها به افراد خاصی محدود می‌کنند. مکانیزم‌های کنترل دسترسی[4] محرمانگی را پشتیبانی می‌کنند. یکی از مکانیزم‌های کنترل دسترسی برای درنظر گرفتن محرمانگی، رمزنگاری[5] است. یک سناریوی ساده از رمزنگاری در شکل ۱-۱ نمایش داده شده است.

علاوه بر محرمانگی اطلاعات، محرمانگی در مورد موجودیت[6] اطلاعات که در مواقعی از خود داده‌ها نیز مهم‌تر است، هم به کار برده می‌شود. به عنوان مثال، ممکن است دانستن این که یک سازمان دولتی چگونه

[1] Confidentiality
[2] Integrity
[3] Availability
[4] Access Control Mechanisms
[5] Cryptography
[6] Existence

شهروندان تحت تابعه خود را آزار داده است، از دانستن این که چنین آزاری اتفاق افتاده مهم‌تر نباشد. در این مورد نیز مکانیزم‌هایی برای جلوگیری از لو رفتن وجود اطلاعات وجود دارد.

یکی از جوانب مهم دیگر محرمانگی، اختفای منابع است. سایت‌ها معمولا تمایل دارند تا پیکربندی و سیستم‌های مورد استفاده خود را از دید دیگران مخفی نگاه دارند و ممکن است سازمان‌ها وجود برخی تجهیزات خاص را از دید دیگران مخفی کنند. برای این نوع محرمانگی نیز مکانیزم‌های خاص دسترسی کنترل وجود دارد.



شکل ۱-۱) استفاده از مکانیزم رمزنگاری برای حفظ محرمانگی

در این شکل کاربر A با استفاده از یک کلید، اطلاعات ارسال شده به کاربر B را از دید کاربر C پنهان می‌کند.

۱-۱-۲ یکپارچگی

یکپارچگی اطلاعات یا منابع، به اعتمادپذیری آنها اشاره می‌کند و معمولا با عنوان جلوگیری از تغییر نامناسب و یا بدون اجازه بیان می‌شود. یکپارچگی شامل یکپارچگی داده (محتویات اطلاعات) و یکپارچگی اصالت (منبعی که داده از آن صادر شده است و اغلب تایید اعتبار[1] نامیده می‌شود) می‌باشد.

مکانیزم‌های حفظ یکپارچگی به دو دسته تقسیم می‌شوند: *مکانیزم‌های جلوگیری* و *مکانیزم‌های کشف*.

مکانیزم‌های جلوگیری[1] با مسدود کردن هر تلاش غیر مجاز برای تغییر داده و نیز هر تلاش برای تغییر داده به یک روش غیرمجاز، به دنبال حفظ یکپارچگی داده‌ها هستند. تفاوت بین این دو نوع تلاش مهم است. در تلاش نوع

[1] Authentication

اول، کاربر می‌کوشد تا داده‌ای که اجازه تغییر آن را ندارد تغییر دهد و در تلاش دوم، کاربری که تنها اجازه تغییر مشخصی را دارد می‌کوشد تا داده را به طرق دیگری که اجازه انجام دادن آنها را ندارد، تغییر دهد. به عنوان مثال یک سیستم حسابداری در یک کامپیوتر را در نظر بگیرید. شخصی به سیستم نفوذ می‌کند و تلاش می‌کند تا داده‌های حسابداری را تغییر دهد. در این صورت یک کاربر غیر مجاز سعی کرده است تا یکپارچگی پایگاه داده حسابداری را نقض کند. حال اگر یک حسابدار که توسط کارفرما استخدام شده است تا کارهای حسابداری او را انجام دهد، سعی کند تا با فرستادن پول به خارج از کشور و پنهان نمودن تراکنش‌ها اختلاس مالی کند، در این صورت تلاش نوع دوم شکل گرفته و یک کاربر مجاز به صورت غیرمجاز داده‌ها را تغییر داده است. تایید اعتبار مناسب و مکانیزم‌های کنترل دسترسی عموما برای جلوگیری از نفوذ افراد غیرمجاز از بیرون استفاده می‌شوند ولی جلوگیری از تلاش نوع دوم نیازمند کنترل‌های پیچیده‌تری است.

مکانیزم‌های کشف[۲] از نقض یکپارچگی جلوگیری نمی‌کنند و در صورت نقض شدن یکپارچگی، تنها گزارش می‌دهند که یکپارچگی داده‌ها دیگر قابل اعتماد نیست. مکانیزم‌های کشف ممکن است برای پیدا کردن مشکلات مربوط به یکپارچگی، رویدادهای سیستم (اعمال کاربر و یا سیستم) و یا تنها خود داده‌ها را مورد تحلیل قرار دهند. همچنین این مکانیزم‌ها ممکن است علت و عاملان نقض یکپارچگی را نیز گزارش کنند و یا فقط دستکاری شدن داده را گزارش دهند.

یکپارچگی داده‌ها با محرمانه بودن آنها بسیار متفاوت است. با بودن محرمانگی، داده یا به خطر افتاده است و یا برای آن مشکلی به وجود نیامده است. اما یکپارچگی، علاوه بر صحیح بودن، قابل اعتماد بودن آن را نیز شامل می‌شود. منبع ارسال کننده داده(چگونه و از چه کسی به دست آمده است)، تا چه اندازه داده قبل از رسیدن به ماشین حاضر مراقبت شده است و تا چه اندازه داده در ماشین حاضر مراقبت می‌شود، همگی یکپارچگی داده را تحت تاثیر قرار می‌دهند. بنابراین ارزیابی یکپارچگی داده معمولا بسیار دشوار است زیرا به فرضیاتی در مورد منبع داده و میزان اعتماد بر آن منبع بستگی دارد.

[1] Prevention Mechanisms
[2] Detection Mechanisms

۱-۱-۳ دسترس‌پذیری

دسترس‌پذیری[1] به توانایی استفاده به موقع از اطلاعات یا منبع خواسته شده اشاره می‌کند. دسترس‌پذیری یکی از جوانب مهم اطمینان‌پذیری[2] و طراحی سیستم است زیرا در دسترس نبودن یک سیستم به معنای آن است که گویا چنان سیستمی وجود ندارد. آن وجه از دسترس‌پذیری که با امنیت در ارتباط است، این است که ممکن است کسی با از بین بردن دسترس‌پذیری یک سیستم، عمداً از دسترسی دیگران به داده و یا سرویس جلوگیری کند. در هنگام طراحی یک سیستم، طراحان سیستم معمولا از یک مدل آماری برای تحلیل الگوهای پیش‌بینی شده‌ی استفاده از سیستم بهره می‌گیرند و مکانیزم‌های آن سیستم را طوری تنظیم می‌کنند، که دسترس‌پذیری تحت آن مدل آماری تضمین شود. با این حال ممکن است شخصی بتواند این الگوهای استفاده (و یا پارامترهایی نظیر ترافیک شبکه که این الگوها را کنترل می‌کنند) را دستکاری کرده و باعث شود که فرضیات آن مدل آماری دیگر صحیح نباشد. این عمل باعث خواهد شد که مکانیزم‌هایی که برای در دسترس نگه داشتن داده و یا منبع در نظر گرفته شده بودند، در محیطی کار کنند که برای کار در آن طراحی نشده‌اند و در نتیجه سیستم از کارکرد صحیح باز ایستد.

تشخیص تلاش برای از بین بردن دسترس‌پذیری، که تحت عنوان حمله ممانعت سرویس[3] نیز نامیده می‌شود، می‌تواند بسیار مشکل باشد زیرا تحلیل‌گر باید تشخیص دهد که الگوهای دسترسی غیرمعمول قابل نسبت دادن به دستکاری عمدی منابع هستند و یا مربوط به تقاضاهای معمولی هستند که در محیط وجود دارند. ماهیت مدل‌های آماری این تشخیص را سخت‌تر می‌کنند زیرا حتی اگر مدل آماری دقیقا محیط را توصیف کند، رویدادهای نابهنجار[4] بخشی از خود مدل آماری خواهند بود و ممکن است گاها اتفاق بیفتند. بنابراین یک تلاش عمدی برای از دسترس خارج ساختن یک منبع ممکن است در بسیاری از موارد همانند یک رویداد نابهنجار به نظر آید[۳].

بزرگترین آسیب وارد شونده از سوی کرم‌های کامپیوتری-که موضوع اصلی این پایان‌نامه می‌باشند- از بین بردن دسترس‌پذیری سیستم‌های مورد حمله است و لذا در ادامه این بخش، این مقوله را مورد مطالعه بیشتری قرار خواهیم داد.

۱-۲ حملات کامپیوتری برای از بین بردن دسترس‌پذیری

[1] Availability
[2] Reliability
[3] Denial Of Service (DOS) attack
[4] Atypical

پس از آنکه سه رکن اصلی امنیت کامپیوتر و شبکه‌های کامپیوتری را ذکر کردیم، در این قسمت به معرفی حملات کامپیوتری برای از بین بردن دسترس‌پذیری سیستم می‌پردازیم. این گونه حملات از این نظر قابل توجه هستند که اصلی‌ترین روش کرم‌ها برای آسیب‌رسانی به سیستم‌های مورد هجوم به شمار می‌آیند.

۱-۲-۱ حملات ممانعت سرویس توزیع‌شده

برای تبیین بیشتر حملات ممانعت سرویس توزیع شده، ابتدا به یک مثال اشاره می‌کنیم. زمانی را به یاد بیاورید که قصد دارید با تلفن تماس بگیرید ولی از آنجا که تمام خطوط شبکه اشغال شده‌اند، قادر به انجام این کار نیستید. این اتفاق ممکن است در برخی ساعات و روزهای خاص که استفاده از تلفن رواج زیادی دارد، اتفاق بیفتد. مثال دیگر در این زمینه، شبکه برق است که در ساعات اولیه شب به علت مصرف فراوان، ناگزیر برق بسیاری از مناطق قطع می‌شود.

اما علت اشغال بودن خطوط و عدم امکان استفاده از سرویس تلفن در این مواقع چه می‌تواند باشد؟ این مشکل از آنجا ناشی می‌شود که شبکه تلفن برای جوابدهی تعداد معدودی از درخواست‌ها در یک زمان طراحی شده است و لذا امکان جواب‌دهی برای تمام درخواست‌ها وجود ندارد. این محدودیت با توجه به ترافیک میانگینی که شبکه دریافت می‌کند (مقدار متوسط درخواست) مشخص می‌شود. اگر مجموع تعداد درخواست‌ها همیشه بالا باشد، آنگاه شرکت مخابرات با احساس این موضوع، ظرفیت پذیرش تقاضا در واحد زمان را افزایش خواهد داد. اما اگر درخواست سرویس میانگین در مقایسه با درخواست سرویس در لحظات پیک کم باشد، آنگاه شرکت مخابرات تنها شبکه‌هایی را خواهد ساخت که نیاز میانگین را جواب بدهند. فراهم آوردن زیرساخت و شبکه لازم برای توانایی پاسخ‌گویی به پیک بار، از دید اقتصادی برای شرکت مخابرات قابل قبول نخواهد بود. در عوض، شرکت مخابرات از مشترکین درخواست می‌کند که از ایجاد بار پیک جلوگیری کنند.

حال تصور کنید که یک مهاجم قصد داشته باشد با حمله به سیستم تلفن، سرویس تماس را برای مشترکین غیر قابل استفاده گرداند. این مهاجم چگونه می‌تواند این کار را انجام دهد؟ یک روش می‌تواند این باشد که این مهاجم با هدف اشغال کردن خطوط شبکه، متناوبا و به صورت پی در پی تقاضای سرویس کند. در این صورت مهاجم باعث خواهد گردید تا منابع شبکه اشغال شود و شرکت مخابرات قادر به پاسخگویی به درخواست‌های مشترکین دیگر نباشد.