به نام آنکه جان را فکرت آموخت

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

دانشکده ریاضی و علوم کامپیوتر

پایان نامه کارشناسی ارشد

مطالعه و بررسی سیستم تشخیص نفوذ هوشمند برای سیستم‌عامل

نگارش
ندا درویش‌زاده

استاد راهنما: دکتر محمد ابراهیم شیری
استاد مشاور: دکتر رضا عزمی

اسفند ۱۳۸۵

بسمه تعالی

دانشگاه صنعتی امیرکبیر
(پلی تکنیک تهران)

فرم اطلاعات پایان نامه
کارشناسی ارشد و دکترا

شماره:

تاریخ:

معاونت پژوهشی

۱-مشخصات دانشجو

نام و نام خانوادگی: ندا درویش‌زاده دانشجوی ■ بورس ☐ مع ☐

شماره دانشجویی : ۸۳۱۱۳۱۶۷ دانشکده : ریاضی و علوم کامپیوتر رشته تحصیلی : علوم کامپیوتر- هوش مصنوعی

نام و نام خانوادگی استاد راهنما : دکتر محمد ابراهیم شیری

عنوان به فارسی : مطالعه و بررسی سیستم تشخیص نفوذ هوشمند برای سیستم عامل

عنوان به انگلیسی : Studying the Intelligent Intrusion Detection System for Operating System

نوع پروژه: کارشناسی ارشد ■ کاربردی ■ بنیادی ☐ توسعه‌ای ■ نظری ☐

دکترا ☐

تاریخ شروع : مهرماه ۱۳۸۴ **تاریخ خاتمه :** ۸ اسفند ماه ۱۳۸۵ **تعداد واحد :** ۶

سازمان تأمین کننده اعتبار :

واژه های کلیدی به فارسی : تشخیص نفوذ - سازوکار هومئوستازیس - شبکهٔ عصبی المن - شبکهٔ عصبی کوهنن - دایمون ممیزی - توابع فراخوان سیستمی

واژه های کلیدی به انگلیسی :
Intrusion detection – Homeostasis – Elman neural network – Kohonen neural network – Auditd daemon – System call

نظرها و پیشنهادها به منظور بهبود فعالیت های پژوهشی دانشگاه :

استاد راهنما :

دانشجو :

امضاء استاد راهنما : **تاریخ :**

نسخه ۱ : معاونت پژوهشی

نسخه ۲ : کتابخانه و به انضمام دو جلد پایان نامه به منظور تسویه حساب با کتابخانه و مرکز اسناد و مدارک علمی

تقدیم به پدر و مادر عزیزم که همواره مشوق و پشتیبان من بوده‌اند.

قدردانی:

خدا را شاکرم که توانستم برگی دیگر از زندگی خویش را با موفقیت به پایان برسانم. از پدر و مادر عزیزم به خاطر حمایتهای بی دریغشان و از اساتید بزرگوارم، جناب دکتر محمد ابراهیم شیری و دکتر رضا عزمی برای راهنماییهایشان سپاسگزارم. از دکتر شیری، به خاطر صبر و حوصله‌شان در پیشرفت پایان‌نامه و از دکتر عزمی، به خاطر ایده‌ها، خلاقیت‌ها و کمک‌هایشان که در تمام مراحل تکمیل ساختار پایان‌نامه، یاری‌ام کرده‌اند؛ سپاسگزارم.

از برادرانم مسعود، امیرعلی و امیرحسین برای همراهی معنویشان، از دوستان عزیزم خانمها ملیحه منصوری و سارا برنجی برای همراهی علمی و حضور سبزشان و نیز از دوست عزیزم سمانه شیرازی برای دلگرمیهایش کمال قدردانی را دارم.

چکیده:

از منظر امنیت کامپیوتر، می‌توان موفقیت سیستم‌های زیستی در حفظ بقاء و پایداری را بعنوان الگوی مناسبی در نظر گرفت. ابزارها و روشهای متداولی که برای تولید سیستم‌های محاسباتی قوی استفاده می‌شوند نمی‌توانند حتی کوچکترین شکل حیات را به شکل مناسب پیاده‌سازی نمایند، در حالیکه سیستم‌های زیستی در طول زمان متکامل شده تا در محیط‌های گوناگون و در مقابل هجومهای مختلف، زنده بمانند و تکثیر شوند.

در این پایان‌نامه سعی شده‌است تا با الهام گرفتن از سازوکار هومئوستازیس مشابه موجودات زنده راه حل نوینی برای سیستم‌های تشخیص نفوذ هوشمند ارایه شود. در این روش، نفوذ به عنوان رفتار غیرعادی برنامه‌ها شناسایی می‌شود و کامپیوترها – مانند سیستم‌های زیستی– بدون نیاز به ابزارهایی از قبیل ضدویروسها، دیواره‌های آتش و غیره می‌توانند از خودشان دفاع کنند. این سیستم‌ها چون قابلیت یادگیری و تشخیص حملات جدید را دارا هستند، نیازمند به روزآوری نمی‌باشند.

سیستم ارایه شده، یک سیستم متمرکز تشخیص نابهنجاری نفوذ مبتنی بر میزبان و تحت سیستم‌عامل لینوکس است. الگوی رفتاری برنامه را بصورت دنباله‌ای پنجاه‌تایی از امضاهای ارایه شده برای توابع فراخوان سیستم تعریف کرده‌ایم بگونه‌ای که هر امضاء شامل هشت فیلد شمارهٔ فراخوانی سیستمی، نتیجهٔ فراخوانی سیستمی، شناسهٔ کاربری، شناسهٔ گروه، euid، egid، suid، sgid است. داده‌های مربوط به الگوهای رفتاری، از گزارش‌های حاصل از زیر سیستم ممیزی سیستم‌عامل لینوکس استخراج شده‌اند. در سیستم پیشنهادی ابتدا با استفاده از شبکه عصبی المن، برنامه‌ها با رفتار غیرعادی، از برنامه‌های عادی تفکیک شده و سپس الگوی رفتاری برنامهٔ غیرعادی به شبکهٔ عصبی کوهنن داده می‌شود تا نوع نفوذ را تشخیص دهد.

کلمات کلیدی:

تشخیص نفوذ – سازوکار هومئوستازیس – شبکهٔ عصبی المن – شبکهٔ عصبی کوهنن – دایمون ممیزی – توابع فراخوان سیستمی

فهرست مندرجات

فصل اول: مقدمه

فصل دوم: مروری بر کارهای پیشین

فصل سوم: مجردسازی سیستم تشخیص نفوذ هوشمند پیشنهادی

فصل چهارم: استخراج الگوی رفتاری برنامه‌ها

فصل پنجم: شبکه‌های عصبی

فصل ششم ساختار سیستم تشخیص نفوذ پیشنهادی

فصل هفتم: نتیجه‌گیری و پیشنهادات

فصل اول : مقدمه

۱-۱- مقدمه

امروزه سیستم‌عامل یکی از بخشهای بنیادین اغلب سیستم‌های کامپیوتری است. تعاریف و کارکردهای مختلفی برای این نرم‌افزار مهم می‌توان ارائه داد به نحوی که توصیف جامع آن در قالب یک عبارت، ناممکن است. از یکسو برخی سیستم‌عامل را یک ماشین مجازی می‌دانند که با فراهم آوردن یک محیط کار جذاب، پیچیدگی‌های سخت‌افزار را از دید برنامه‌نویس و کاربران پنهان می‌کند[۱]. از سوی دیگر می‌توان آنرا مدیر منابع سیستم دانست که وظیفه خطیر به اشتراک گذاشتن منابع بین پردازه‌ها را بر عهده دارد. آنچه مسلم است این است که سیستم‌عامل نرم‌افزاری بزرگ با ساختاری پیچیده است و در شرایطی که مفاهیمی چون چند برنامگی، همزمانی، امکان اشتراک منابع سیستمی و توزیع‌پذیری به عنوان بخشی از سرویس‌های سیستم مطرح است، مقوله امنیت در این نرم‌افزار اهمیت حیاتی یافته و بسیار مورد توجه قرار می‌گیرد.

امنیت سیستم عامل حول چهار مفهوم حفاظتی *محرمانگی*، *جامعیت داده‌ها*، *در دسترس بودن* و نهایتاً *تعیین اعتبار* یا *احراز هویت* تعریف می‌شود.

برای آنکه درک مشترکی از مطالب ارائه شده در فصل‌های بعدی بدست آید، لازم است برخی مفاهیم و تعاریف اولیه مورد بررسی قرارگیرد. با این مقدمه دراین فصل، ابتدا به تعریف مفاهیم اولیه امنیت می‌پردازیم، سپس به بررسی مفهوم امنیت در سیستم‌عامل پرداخته و ضمن شناخت خطرات مشترک بین سیستم عامل‌های امروزی، ملاحظات امنیتی که برای یک سیستم عامل امن متداول است را بیان می‌کنیم، در پایان هدف از این پایان‌نامه را به تفصیل شرح داده و ساختار پایان‌نامه را مشخص می‌کنیم.

۱-۲- مفاهیم اولیه امنیت

برای آنکه درک مشترکی از مطالب ارائه شده در فصل‌های بعدی بدست آید، لازم است برخی مفاهیم و تعاریف اولیه مورد بررسی قرار گیرد.

۱-۲-۱- سرویس‌های اساسی درجهت تامین امنیت

سرویس‌های اساسی درجهت تامین امنیت در سیستم‌های کامپیوتری را می‌توان به چند دسته تقسیم کرد:

- **محرمانگی**[1] به معنای منع یا محدود کردن دسترسی و مشاهده اطلاعات به شکل غیرمجاز می‌باشد.

- **جامعیت داده‌ها**[2] بدین مفهوم است که داده‌هایی که با آنها سر و کار داریم همان داده‌های مورد نظر، واقعی و غیرمخدوش هستند.

- **در دسترس بودن**[3] به مفهوم آنکه منابع سیستم برای کاربر مجاز که قصد دستیابی و استفاده از آنها را دارد مهیا باشد.

- **تعیین اعتبار** یا **احراز هویت**[4] به معنای آنکه سیستم قادر به تشخیص هویت کاربر خود باشد.

۱-۲-۲- تهدید

افزایش نیاز به دسترسی به داده‌ها و پردازش سریع‌تر آنها و در عین حال افزایش حجم داده‌ها و نیاز به فراهم آوردن داده‌ها از منابع مختلف از طریق شبکه‌های کامپیوتری، منجر به پدید آمدن منابع تهدیدآمیزی گردیده است که از طریق نقاط ضعف موجود در آن‌ها، می‌توان به استثمار سیستم‌ها و ایجاد اختلال در آن‌ها پرداخت [۲].

به طورکلی، **تهدید**[5] عبارت است از هر وضعیت یا اتفاقی که قابلیت ضرر زدن به سیستم را داشته باشد. این ضرر می‌تواند به صورت انکار، افشاء، خرابی یا تغییر داده‌ها و منابع سیستم باشد.

---

[1] Confidentiality
[2] Integrity
[3] Availability
[4] Authentication
[5] Threat

یک تهدید ممکن است از سوی منبعی انسانی باشد، مانند یک دسترسی غیرمجاز توسط یک فرد به اطلاعاتی خاص، یا از سوی منبعی فیزیکی، نظیر حوادثی چون سیل، آتش‌سوزی و قطع برق و یا از سوی منبعی کامپیوتری، مثل ویروس‌ها و حملهٔ اسب‌های تروایی[6] باشد. تهدیدات می‌توانند داخلی و یا خارجی باشند. همچنین می‌توانند عمدی و یا غیرعمدی رخ دهند.

یک دسته‌بندی از جیمز اندرسون در رابطه با تهدیدات کامپیوتری به ترتیبی است که در زیر آمده است[۳و٤] :

- **نفوذگران[7] خارجی**: کسانی که مجاز به استفاده از کامپیوتر مربوطه نیستند.

- **نفوذگران داخلی**: کسانی که مجاز به استفاده از کامپیوتر هستند اما حق استفاده از داده‌های خاصی را ندارند. این تهدیدات داخلی خود به دو دسته تقسیم می‌گردند:
  - **نقابداران**[8]: آنهایی که با سرقت هویت و اعتبار دیگران وارد سیستم می‌گردند.
  - **کاربران نامشروع**[9]: آنهایی که به طور موفق معیارهای نظارت و ممیزی را تجاهل نموده و آن‌ها را دور می‌زنند.

- **سوءاستفاده‌گرها**[10]: کسانی که هم حق استفاده از کامپیوتر و هم حق استفاده از داده‌ها را دارند اما از حقوق خود سوء استفاده می‌کنند.

۱-۲-۳- آسیب‌پذیری

آسیب‌پذیری[11] عبارت است از ضعف در رویه‌های امنیتی خودکار، رویه‌های مدیریتی[12] و یا رویه‌های کنترلی داخلی که به وسیلهٔ یک تهدید در جهت دسترسی غیر مجاز به اطلاعات و یا از هم گسیختگی یا انقطاع در یک پردازش حساس و حیاتی، مورد بهره‌برداری و استثمار قرار می‌گیرد. به نقاط آسیب‌پذیری یک سیستم حفرهٔ امنیتی[13] سیستم نیز گویند [۵].

جیمز اندرسون یک آسیب پذیری را با سطح انتزاعی پایین‌تر بدین صورت تعریف می‌نماید که آسیب پذیری عبارت است *از درز یا رخنهٔ شناخته شده و یا مشکوک در طراحی یا عملکرد سخت‌افزار یا نرم‌افزار یک سیستم که موجب نفوذ در اطلاعات آن سیستم می‌گردد.*

---

[6] Trojan Horses Attack
[7] Penetrator
[8] Masqueraders
[9] Clandestine Users
[10] Misfeasor
[11] Vulnerability
[12] Administrative
[13] Security Hole

ضعـف‌ها و نقاط آسیب‌پذیری سیستم‌ها را می‌توان به طور کلی به دو دسته زیر تقسیم نمود[۲]:

- ضعف در طراحی و پیاده‌سازی نرم‌افزار یا سخت‌افزار سیستم، که به حفره‌های فنی سیستم معروفند.
- ضعف در سیاست امنیتی، پیکربندی، کنترل یا مدیریت سیستم، که به آن‌ها حفره‌های مدیریتی گویند.

باید توجه داشت که تهدید و آسیب‌پذیری ذاتاً با یکدیگر در ارتباطند، چرا که تهدید، نتیجهٔ سوء استفاده از یک یا چند حفرهٔ امنیتی یا نقاط آسیب‌پذیری در یک سیستم می‌باشد.

۱-۲-۴- تهاجم

در لغت نامه‌ها تعاریف مختلفی برای **تهاجم**[14] یا نفوذ آمده است و این در حالی است که در مباحث امنیتی کامپیوتر تعریف ثابتی برای این مفهوم وجود ندارد. بسیاری معتقدند که تهاجم به معنای حملات ناموفق می‌باشد و این در حالی است که برخی دیگر حمله را جدای از نفوذ می‌دانند. در [۵] تهاجم بصورت زیر تعریف شده است:

به هر مجموعه از اعمالی که هدف آن نقض جامعیت، محرمانگی یا دسترس‌پذیری یک منبع باشد، تهاجم یا نفوذ گفته می‌شود. این تعریف تمام انواع تهدیدات را در بر می‌گیرد. در این پایان‌نامه تهاجم را بصورت زیر تعریف می‌کنیم:

تهاجم یک رشته فعالیتهای عمدی است که جهت آزار و صدمه رساندن صورت می‌پذیرد مانند غیر قابل استفاده نمودن یک سیستم، دسترسی غیر مجاز به اطلاعات و یا دستکاری اطلاعات. در این تعریف هر گونه تلاش موفق و ناموفق مورد نظر می‌باشد.

برای وارد کردن خسارت به جامعیت یا محرمانگی اطلاعات، لازم است که مهاجم یا حمله‌کننده در ابتدای امر به سیستم حاوی اطلاعات دسترسی داشته باشد و لذا اولین گام در این‌گونه تهاجم‌ها، دسترسی به سیستم هدف می‌باشد، ولی تهاجمی که به دسترس‌پذیری سیستم خسارت وارد می‌کند، معمولاً نیازی به دسترسی به سیستم به عنوان پیش نیاز حمله خود ندارد [٦].

۱-۳- امنیت در سیستم‌عامل

امکان آسیب‌پذیری در اکثر سیستمهای نرم‌افزاری بزرگ و پیچیده وجود داشته و حداقل با امکانات نرم‌افزاری متدها، ابزارها و تکنیکهای امروزی امکان حذف کامل رخنه‌های نفوذ به این سیستمها

[14] Intrusion

وجود ندارد. سیستم‌عاملها نیز از جمله نرم‌افزارهای بزرگ و پیچیده و به تبع آن آسیب‌پذیر هستند. هرروزه گزارشات زیادی مبنی بر کشف آسیب‌پذیریهای نرم‌افزاری و بخصوص سیستم‌عاملها داده می‌شود که با نصب بسته‌های[15] جدید می‌توان احتمال رخداد حمله‌ها را کاهش داد. با این وصف تلاشهای بسیاری در جهت افزایش امنیت این قبیل سیستمهای نرم‌افزاری صورت گرفته است که بسیاری از مکانیزمهای حفاظتی نظیر احراز هویت، کنترل دسترسی و ... از جمله این دستاوردهای پدید آمده در توسعه سیستم‌عاملها است.

۱-۳-۱- آسیب‌های امنیتی سیستم‌عامل‌ها

مهاجمان در ابتدای کار برای پیدا کردن دسترسی به دنبال آسیب‌پذیری می‌گردند. سپس به دنبال آسیب‌پذیری‌های سیستم‌عامل و ابزارهای اسکنی می‌گردند که آن آسیب‌پذیری‌ها را گزارش دهد. پیداکردن آسیب‌پذیری‌های خاص در یک سیستم‌عامل، به راحتی تایپ یک آدرس URL و کلیک بر روی لینک مناسب می‌باشد. سازمان‌های بسیاری وجود دارند که اطلاعات "آشکارکننده کاملی[16]" را فراهم می‌آورند. آشکار کننده کامل تکنیکی است که در آن تمامی اطلاعات در اختیار حوزه عمومی قرار داده می‌شود. به این ترتیب دیگر این اطلاعات تنها برای جامعه هکرها شناخته شده نخواهد بود.

میتر[17] یک گروه دولتی در آمریکا است که از یک دیکشنری آسیب‌پذیری‌های معمول و آشکارسازی[18] آنها پشتیبانی می‌نماید. هدف آنها تهیه یک لیست از اسامی استاندارد شده برای آسیب‌پذیری-ها و دیگر اطلاعات آشکارساز امنیتی می‌باشد. سایت‌های امنیتی دیگر، نظیر SecurityFocus[19]، CERT[20]، مؤسسهٔ SANS[21] و بسیاری دیگر، اطلاعاتی درباره چگونگی تعیین آسیب‌پذیری‌های یک سیستم‌عامل و بهترین راه آشکارسازی آنها را در اختیار عموم قرار می‌دهند. بنابراین، دسترسی به یک سیستم ناامن حتی برای یک هکر تازه‌کار بسیار ساده خواهد بود.

با استفاده از یک موتور جستجو و شماره CVE، که از طریق جستجو در سایت میتر بدست می-آید، این امکان فراهم می‌گردد که کد منبع و دستورات دقیق چگونگی استفاده از آن را پیدا نمائید. کل فرآیند تنها چند دقیقه به طول می‌انجامد. هکر می‌تواند کد منبع را از وب سایت SecurityFocus پیدا کرده و دستورات دقیق چگونگی استفاده از آن را در سایت SANS جستجو نماید.

---

[15] patch
[16] Full disclosure
[17] Mitre: http://cve.mitre.org/
[18] Common Vulnerability and Exposures (CVE)
[19] www.securiryfocuse.com
[20] www.cert.org
[21] http://www.sans.org/

صرفه‌نظر از ضعفها و رخنه‌هایی که ممکن است هر یک از سیستم‌عاملهای امروزی داشته باشند، منشأ اکثر تهدیدات جدی که بطور مشترک متوجه اغلب سیستم‌عاملها می‌باشد یکی از پنج عاملی است که ذیلاً به شرح آنها خواهیم پرداخت.

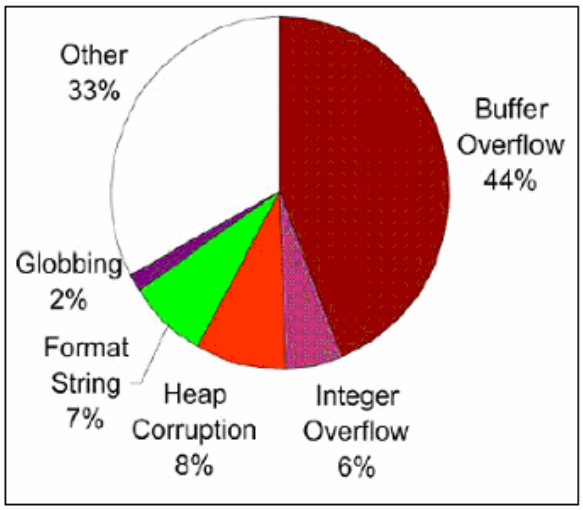
۱-۳-۱-۱- تصدیق ورودی نامعتبر

کنترل دقیق ورودی روتینهای نرم‌افزاری از اهمیت بالایی برخوردار است. این کنترل می‌تواند بر روی تعداد پارامترهای ورودی و یا نوع هر پارامتر باشد. همچنین ممکن است کنترل شود که میزان داده ورودی از حجم بافر اختصاص داده شده به آن بیشتر نباشد.

تصدیق اعتبار داده نامعتبر و ناموجود یکی از معضلات شناخته شده و جدی سیستم‌عاملها است. بعنوان مثال تعیین اعتبار پارامترهای ورودی هریک از توابع سیستمی آنقدر با اهمیت است که اقتضا می‌کند این توابع در مد هسته اجرا شوند. با این حال تمامی سیستم‌عاملها از جمله ویندوز NTکنترل دقیقی بر روی پارامترهای فراخوانی سیستمی ندارند.

یک نمونه دیگر سرریزبافر[۲۲] در پیاده‌سازی پروتکلها است که معضل مشترک اکثر سیستم‌عاملهای مبتنی بر شبکه تلقی می‌شود. در سالهای اخیر اسکریپت‌های فراوانی ارائه شده‌اند که از این ضعف سیستم‌عاملها بهره می‌برند. Trapdor، Bonk، Boink و Land نمونه‌هایی از این دسته اسکریپتها هستند [۷]. با وجود سالها هنوز سرریز بافر بیشترین آسیب‌پذیری گزارش شده در سیستم‌عاملها می‌باشد [۸] (شکل ۱-۱).

[22] buffer overflow



شکل(۱-۱): آماری از آسیب‌پذیری‌های موجود که منجر به نفوذ در سیستم‌ها شده است.

۱-۳-۱-۲- ضعف در الگوریتم های رمزنگاری

یکی دیگر از معضلات امنیتی سیستم‌عاملها، ضعف در الگوریتمهای رمزنگاری مورد استفاده آنها است. در سیستم‌عاملها از الگوریتمهای رمزنگاری برای رمزکردن کلمات عبور استفاده می‌شود. بنابراین اگر الگوریتمی که مورد استفاده قرار می‌گیرد به میزان کافی قدرتمند نباشد ممکن است نفوذگران بتوانند با تحلیل آن، کلمه رمز را تشخیص داده و بازخوانی کنند.

باید توجه داشت که حتی الگوریتمهای کارآمد نیز ممکن است پس از مدتی ناگهان با دستیابی به روشهای کشف آن، کارآیی خود را از دست بدهند.

به عنوان مثال در ویندوز NT کلمه عبور در دو مرحله رمز می‌شود یکی در قالب مدیر شبکه (LM) و دیگری فرمت محلی NT. کلمه عبور در مرحله رمزنگاری LM در صورتی که کمتر از ١٤ کاراکتر داشته باشد توسط کاراکتر پوچ پر می‌شود. حال چنانچه سایز کلمه رمز کمتر از ۸ کاراکتر باشد امکان رمزگشایی و کشف کلمه عبور وجود خواهد داشت. چرا که در اینصورت تعداد تلاشهای لازم برای بازشناسی رمز، کم شده و قابل اجرا خواهد بود.

۱-۳-۱-۳- ضعف در پروتکلهای احراز هویت

پیش از آنکه هر کاربری امکان دسترسی به منابع یک سیستم را بدست آورد، لازم است موجودیت خود را برای سیستم به اثبات برساند. این فرآیند احراز هویت نامیده می‌شود. غالب سیستمهای احراز هویت مبتنی بر استفاده از یک رمز مشترک بین بخشهای درگیر در این فرایند هستند بطوریکه در مکانیزم احراز

هویت یک کلمه رمز بین سیستم و کاربر بطور مشترک و محرمانه وجود خواهد داشت. بخش اصلی کار که محل بروز مشکل است پیاده سازی یک روال احراز هویت امن است. پیاده‌سازی این روال، بخصوص در محیطهای توزیع شده یک پروسه پیچیده محسوب می‌شود.

یک مورد از این دست آسیب‌پذیری، نوعی حمله است که بطور مشابه در سرویس دسترسی از راه دور ویندوز NT و نیز سرویس سیستم اطلاعات شبکه[۲۳] بکار رفته در محیط سیستم‌عامل تحت شبکه یونیکس رخ می‌دهد. در این شیوه، حمله کننده با فریب یک مشتری، خود را به عنوان سرویس دهنده به او معرفی می‌کند. در هر دو مورد ذکر شده به دلیل ضعف سیستم عامل در روال احراز هویت، مشتری ناآگاهانه بدون آنکه تشخیص دهد سرور واقعی است یا خیر، اطلاعات خود را در اختیار او قرار می‌دهد [۹و۱۰].

یک نمونه دیگر از این قبیل ضعفها باز به سیستم عامل ویندوز NT باز می‌گردد. این سیستم عامل از ۸ نوع احراز هویت با سطوح امنیتی متفاوت پشتیبانی می‌کند. سرویس‌دهنده و مشتری از طریق گفتگو با یکدیگر متد احراز هویتی که باید مورد استفاده قرار دهند را انتخاب می‌کنند. از آنجا که بطور پیش فرض سرویس‌دهنده کلمه عبور شفاف و رمز نشده را بعنوان متغیر احراز هویت معتبر می‌شناسد، گاهاً ممکن است یک نفوذگر با فریب مشتری در گفتگوی او با دیگر بخشهای ارتباط وارد شود و او را به استفاده از متغیر احراز هویت به صورت شفاف تحریف کند و از این طریق به هنگام انتقال کلمه عبور، به آن دست یابد. در این حالت هیچ یک از بخشهای ارتباط متوجه حمله نخواهند شد [۱۱].

۱-۳-۱-٤- راه اندازی نامطمئن

واضح است که در سیستم عاملهای امروزی راه اندازی اولیه سیستم یک مسأله امنیتی بسیار مهم است و اغلب سیستم عاملهایی که مورد ارزیابی قرار گرفته اند، در مرحله راه اندازی اولیه آسیب‌پذیر بوده‌اند.

بعنوان مثال سیستم عامل سان[۲٤] به سادگی در مد کاربر بازآغازی[۲۵] می‌شود و یا اینکه دستورات در مد کاربر با حق دسترسی ریشه[۲٦] اجرا می‌شوند.

همچنین هنگامی که ویندوز NT بر روی یک کامپیوتر اجرا می‌شود این مسأله وجود دارد که یک سیستم‌عامل بیرونی می‌تواند آن را دوباره راه‌اندازی کند. هنگامیکه سیستم عامل بیرونی بر روی کامپیوتر مذکور راه‌اندازی شد دیگر مکانیزم کنترل دسترسی به فایلهایی که بر روی یک پارتیشن با سیستم فایل NTFS واقع است، مبتنی بر سیستم عامل ویندوز NT نخواهد بود.

[23] Network Information System(NIS)
[24] Sun
[25] restart
[26] root

۱-۳-۱-۵- خطاهای پیکربندی

در سیستم‌عاملهای فعلی اغلب، مکانیزمها و قابلیتهای امنیتی بطور پیش فرض فعال نمی‌شوند. برای دسترسی به سطوح امنیتی لازم است مالک سیستم پس از آنکه سیستم‌عامل را بطور کامل نصب کرد، به امن کردن سیستم بپردازد. اما از آنجا که سیستم عاملها، نرم‌افزارهای بزرگ و پیچیده‌ای هستند، پیکربندی امنیتی آنها کار ناچیز و ساده‌ای نیست. بعلاوه اینکه تعداد افراد توانمند در بحث امنیت کامپیوتر محدود است.

در نسخه‌های اولیه سیستم‌عامل نت‌ور[۲۷] جعل کردن بسته‌های NCP که بین مشتریها و سرویس‌دهنده رد و بدل می‌شد کار ساده‌ای بود. از این رو ناول مفهوم امضای بسته را در نسخه ۳،۱۲ سیستم‌عامل عرضه کرد. اما متأسفانه این قابلیت امنیتی بطور پیش فرض و با نصب سیستم‌عامل فعال نمی‌شد. به همین ترتیب در اغلب نسخه‌های اخیر نت ور نظیر نت ور نسخه ۵ نیز نصب سرویس امضای بسته‌ها تنها بر اساس درخواست طرف مقابل انجام می‌گیرد. این مسأله سبب می‌شود که اگر مشتری و سرویس‌دهنده از نصب پیش فرض استفاده نمایند، بسته‌ها امضا نشوند و لذا سیستم به لحاظ امنیتی آسیب‌پذیر باشد.

همچنین در نسخه اولیه سیستم‌عامل سان دایرکتوری پایگاه‌داده پیکربندی سرویس‌دهنده سیستم اطلاعات شبکه، حق دسترسی مد ۰۷۷۷ داشت. بدین مفهوم که مالک، گروه و یا هر کاربری امکان خواندن، نوشتن و اجرا کردن در این دایرکتوری را داشتند. با این پیکربندی بسیار خطرناک، طبیعتاً هر کسی می‌تواند یک کاربر و یا گروه جدید ایجاد و یا کاربر یا گروهی را حذف کند [۱۲] .

۱-۳-۲- مکانیزمهای حفاظت در سیستم‌عامل

در [۱۳] نوعی تعریف از حفاظت در سیستم عامل ارائه شده است. در این تعریف، تفکیک به عنوان اساس حفاظت مطرح شده و این تفکیک در چهار سطح فیزیکی، موقت، منطقی و تفکیک مبتنی بر رمزنگاری تشریح شده است.

دسته بندی دیگری نیز از قابلیت حفاظت سیستم عامل مطرح شده که در آن سیستم، حفاظت را به یکی از اشکال زیر اعمال می‌کند [۱٤]:

۱- سیستم بدون حفاظت

در این روش سیستم عامل با اجرای روالهای حساس در زمانهای جداگانه از آنها محافظت می‌کند.

---

[27] NetWare

۲- ایزوله کردن

در این رویکرد، هر پردازه‌ای بطور مجزا از دیگر پردازه‌ها اجرا می‌شود بدون آنکه هیچگونه اشتراک منابعی بین آنها وجود داشته باشد. در این روش هر پردازه مستقل از دیگران فضای حافظه، فایلها و دیگر منابع خاص خود را دارد.

۳- اشتراک همه یا هیچ

در این روش، صاحب هر شیء که قرار است به اشتراک گذاشته شود مشخص می‌کند که این شیء اختصاصی است یا عمومی. به‌عبارت دیگر مالک شیء است که می‌تواند شیء را در دسترس پردازه‌های خود قرار دهد.

٤- اشتراک تحت یک حریم دسترسی

در این شیوه، سیستم‌عامل است که توانایی دسترسی یک کاربر به شیء خاصی را بررسی و کنترل می‌کند. بنابراین سیستم‌عامل در این بین نقش محافظ را ایفا می‌نماید و اطمینان می‌دهد که تنها دسترسی‌های مجاز رخ خواهد داد.

۵- اشتراک بر محور قابلیت پویا

این رویکرد روشی توسعه یافته‌تر از روش کنترل دسترسیها (روش قبل) است که البته امکان تعریف پویای حقوق دسترسی بر اشیاء را فراهم می‌آورد.

٦- محدودیت در نوع استفاده از اشیاء

در این شکل از حفاظت، سیستم عامل نه تنها دسترسی به اشیاء بلکه شیوه استفاده از آنها را کنترل می‌کند.

با این تعاریف، هر سیستم عاملی ممکن است برای اشیاء مختلف درجات متفاوتی از حفاظت را اعمال کند. آنچه مسلم است این است که باید سیستم عامل بین دو مقوله اشتراک منابع و حفاظت از منابع هر کاربر نوعی توازن ایجاد کند.

برای تبیین بهتر آنچه در قالب روشهای اعمال حفاظت ارائه شد، حافظه را بعنوان یکی از منابع سیستم مورد بررسی قرار می‌دهیم. در محیط چند برنامه‌ای حفاظت از حافظه اصلی، مسأله بسیار مهمی است. در این خصوص نه تنها امنیت داده‌ها بلکه عملکرد صحیح پردازه‌ها در دسترسی به حافظه نیز باید مورد توجه قرارگیرد. تفکیک در حافظه اصلی می‌تواند به سادگی با استفاده از طرح حافظه مجازی مبتنی بر صفحه بندی یا قطعه بندی و یا ترکیبی از این اعمال شود. اگر ایزوله کردن کامل برای حفاظت مدنظر باشد (دومین متد حفاظت که پیش از این معرفی شد) کافی است در تخصیص فضا به پردازه‌ها، سیستم‌عامل