دانشگاه شهید بهشتی
دانشکده مهندسی برق و کامپیوتر

معماری سخت‌افزاری کارا برای سیستم‌های تشخیص نفوذ ترکیبی

پایان نامه کارشناسی ارشد مهندسی کامپیوتر
گرایش معماری کامپیوتر

محمد امین طاهرخانی

استاد راهنما:
مقصود عباسپور

۱۳۸۸

دانشگاه شهید بهشتی

دانشکده مهندسی برق و کامپیوتر

پایان نامه کارشناسی ارشد مهندسی کامپیوتر - گرایش معماری کامپیوتر

تحت عنوان:

معماری سخت‌افزاری کارا برای سیستم‌های تشخیص نفوذ ترکیبی

در تاریخ پایان نامه ، محمد امین طاهرخانی، توسط کمیته تخصصی داوران مورد بررسی و تصویب نهـائی قرار گرفت.

۱- استاد راهنما:	نام ونام خانوادگی: دکتر مقصود عباسپور	امضاء
۲-استاد داور (داخلی)	نام ونام خانوادگی: دکتر محمد عشقی	امضاء
۳- استاد داور (خارجی)	نام ونام خانوادگی: دکتر احمد خوانساری	امضاء
۴- نماینده تحصیلات تکمیلی	نام ونام خانوادگی: دکتر فرح ترکمنی آذر	امضاء

کلیه حقوق مادی مترتب بر نتایج مطالعات،

ابتکارات و نوآوریهای ناشی از تحقیق موضوع

این پایان نامه متعلق به دانشگاه شهید بهشتی

می باشد.

به نام خدا

نام ونام خانوادگی: محمد امین طاهرخانی
عنوان پایان نامه: معماری سخت‌افزاری کارا برای سیستم‌های تشخیص نفوذ ترکیبی
استاد راهنما: دکتر مقصود عباسپور

اینجانب **محمد امین طاهرخانی** تهیه کننده پایان نامه کارشناسی ارشد حاضر، خود را ملزم به حفظ امانت داری و قدردانی از زحمات سایر محققین و نویسندگان بنا بر قانون حق تالیف (Copyright) می دانم. بدین وسیله اعلام می نمایم که مسئولیت کلیه مطالب درج شده با اینجانب می باشد و در صورت استفاده از اشکال؛ جداول، و مطالب سایر منابع، بلافاصله مرجع آن ذکر شده و سایر مطالب از کار تحقیقاتی اینجانب استخراج گشته است و امانتداری را به صورت کامل رعایت نموده ام. در صورتی که خلاف این مطلب ثابت شود، مسئولیت کلیه عواقب قانونی با شخص اینجانب می باشد.

نام ونام خانوادگی: محمد امین طاهرخانی

امضاء وتاریخ:

تقدیم به پدر و مادر عزیزم

فهرست مطالب

فهرست اشکال

فهرست جداول

چکیده

سیستم‌های تشخیص نفوذ به عنوان یکی از ابزارهای کارآمد برای برقراری امنیت در سامانه‌های فناوری اطلاعات شناخته می‌شوند. فرصت ارائهٔ سرویس‌های متنوع از طریق شبکه در برابر تهدید افزایش تعداد و پیچیدگی تهاجمات و همچنین مسئلهٔ افزایش سرعت شبکه‌ها از دلایلی می‌باشند که اعمال روش‌های کارا در تشخیص نفوذ را به یک ضرورت تبدیل نموده است. طراحی و پیاده‌سازی معماری‌های سخت‌افزاری برای رفع گلوگاه سیستم‌های تشخیص نفوذ و افزایش کارایی آن یک ایده مناسب می‌باشد که در پژوهش‌های معتبر متعددی به آن پرداخته شده است. در این پژوهش با تحلیل معماری‌های سخت‌افزاری پیشین و ارزیابی نقاط قوت و ضعف ساختارهای کلاسیک مبتنی بر آن، یک معماری سخت-افزاری کارا برای سیستم‌های تشخیص نفوذ ترکیبی (دورگه) ارائه می‌شود که قابلیت تشخیص فرم‌های مختلف را از تهاجمات شناخته شده و ویرایش شده تا ناهنجاری‌های مربوط به پروتکل‌ها و برنامه‌های کاربردی داراست. پیچیدگی زمانی حداقلی در پردازش الگوهای تهاجمات به همراه دقت و صحت بالا در تشخیص تهاجمات از جمله ویژگی‌های معماری پیشنهادی می‌باشد.

کلمات کلیدی: تشخیص مبتنی بر سوءاستفاده، تشخیص مبتنی بر ناهنجاری، تطبیق الگوی تهاجمات، معماری سخت-افزاری، حافظه‌های آدرس‌پذیر محتوا، بازرسی عمیق بسته‌ها

فصل ۱) مقدمه

با اینکه ایدهٔ ایجاد سیستم‌های تشخیص نفوذ به سالها قبل باز می‌گردد، اما با گستردگی شبکه‌های کامپیوتری و ارائهٔ سرویس‌های متنوع توسط سازمان‌ها، ادارات و شرکت‌های بزرگ و کوچک و همچنین مطرح شدن مباحث نوین فناوری اطلاعات نظیر دولت الکترونیک، تجارت الکترونیک، انتخابات الکترونیک، استفاده از این ابزار مفید به عنوان یکی از مولفه‌های برقراری امنیت بسیار مورد توجه قرار گرفته است. به دلیل اهمیت سیستم‌های تشخیص نفوذ برای کشف حملات بر روی منابع و سرمایه‌های اطلاعاتی، این ابزارها دارای جایگاه ویژه‌ای در برقراری امنیت شبکه‌ها می‌باشند.

اعتبار این ابزارهای امنیتی هنگامی دو چندان می‌شود که روند صعودی افزایش مخاطرات امنیتی مورد تحلیل قرار گیرد. از مهمترین دلایل این مسئله، افزایش تعداد تهاجمات و در عین حال پیچیده‌تر شدن آنها می‌باشد. شکل ۱-۱ نمونه‌ای را از آمار رخدادهای امنیتی گزارش‌شده در CERT/CC [1] از سال ۱۹۸۸ (سال شروع فعالیت این گروه) تا سال ۲۰۰۳ (آخرین اعلام رسمی این گروه برای ارائهٔ تعداد رخدادها) نشان می‌دهد. همانطور که ملاحظه می‌شود رخدادهای امنیتی گزارش شده در طی آن سال‌ها به صورت چمشگیری افزایش یافته است. این شرایط در سایر مراکز معتبر امداد حوادث رایانه‌ای[۱] و تیم‌های پاسخ به حوادث امنیتی رایانه‌ای[۲] نیز در طی سال‌های اخیر گزارش شده است. به عنوان نمونه می‌توان به آمارهای ارائه شده توسط گروه‌های MyCERT [۳] و CERT.br [۴] اشاره کرد. شکل ۱-۲ تعداد رخدادهای امنیتی گزارش شده در این دو مرکز را بین سال‌های ۲۰۰۰ تا ۲۰۰۸ نشان می‌دهد [2]-[3]. همانطور که ملاحظه می‌شود تعداد رخدادهای امنیتی گزارش شده در طی این ۹ سال برای MyCERT و CERT.br به ترتیب بیش از ۱۶۴ و ۳۷ برابر شده‌است.

علاوه بر افزایش تعداد رخدادهای امنیتی، می‌بایست مسئله افزایش پیچیدگی تهاجمات در طراحی و توسعهٔ سیستم‌های تشخیص نفوذ مورد توجه قرار گیرد. ابزارهای هوشمند تهاجم با بهره‌برداری از پایگاه‌های دانش آسیب‌پذیری‌ها و تهاجمات، می‌توانند هر مهاجمی را با هر سطحی از دانش در زمینه امنیت شبکه به جهت اجرای فعالیت‌های ناهنجار و

---

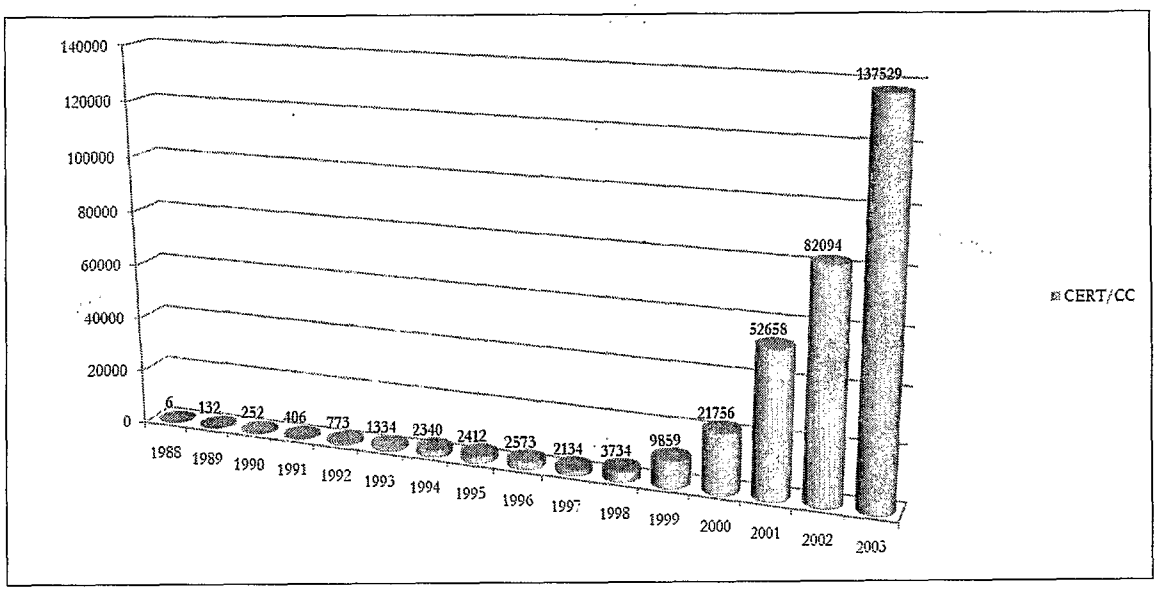
[۱] Computer Emergency Response Team - CERT

[۲] Computer Security Incident Response Team - CSIRT

[۳] MyCERT گروه امداد حوادث رایانه‌ای مالزی و عضو مجمع گروه‌های امنیتی و پاسخ به حوادث (FIRST) می‌باشد.

[۴] CERT.br گروه امداد حوادث رایانه‌ای در برزیل و عضو مجمع گروه‌های امنیتی و پاسخ به حوادث (FIRST) می‌باشد.

تهاجمات پیچیده مجهز نماید. علاوه بر این، با گسترش کاربرد فایروال‌ها و سیستم‌های تشخیص و یا پیش‌گیری از نفوذ، روش‌های فریب و گریز[۱] از تشخیص و پالایش در این ابزارها به جهت دور زدن[۲] آنها توسط مهاجمین مورد استفاده قرار گرفته است. در نتیجهٔ اعمال تکنیک‌های گریز از تشخیص و پالایش در توسعهٔ این ابزارها، فرآیند تشخیص نفوذ دشوارتر شده است.



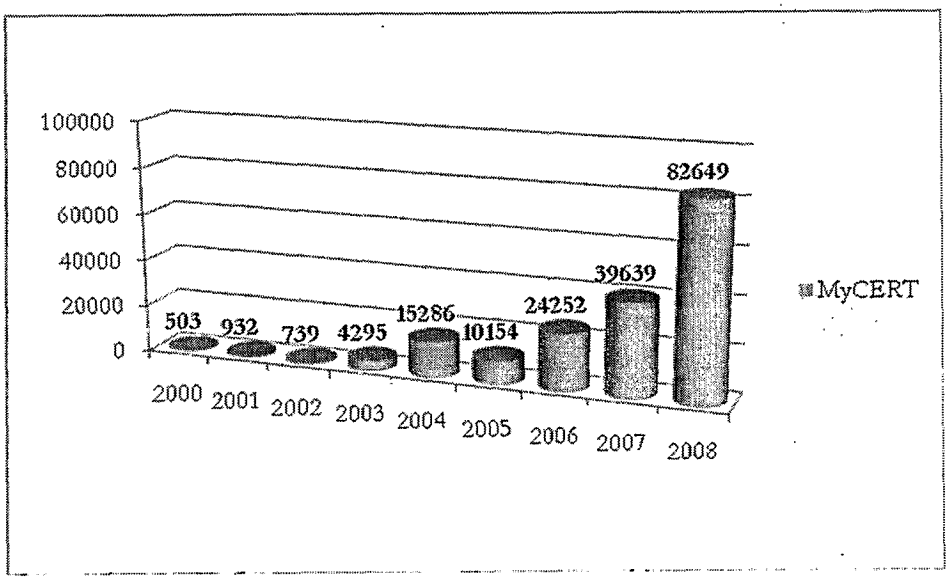
شکل ۱-۱ آمار منتشر شدهٔ CERT/CC از تعداد رخدادهای امنیتی

از سویی دیگر، مسئله افزایش سرعت شبکه‌های رایانه‌ای و افزایش حجم منابع ورودی به جهت پردازش و ارائه خدمات به دغدغهٔ دیگری برای مدیران شبکه‌ها تبدیل شده است. ارائهٔ خدمات به کاربران در حداقل زمان ممکن و با کیفیت مناسب و به طبع آن رضایت مشتریان جزو اهداف سازمان‌ها و شرکت‌ها می‌باشد. بنابراین در اعمال مکانیزم‌های امنیتی (از جمله جلوگیری، تشخیص و پاسخ به نفوذ) مسئله کشف فعالیت‌های غیرمجاز از میان انبوهی از تراکنش‌های کاربران با حداقل تاثیر جانبی در پردازش فعالیت‌های مجاز کاربران می‌بایست به عنوان یک نیاز اساسی مورد توجه قرار گیرد.

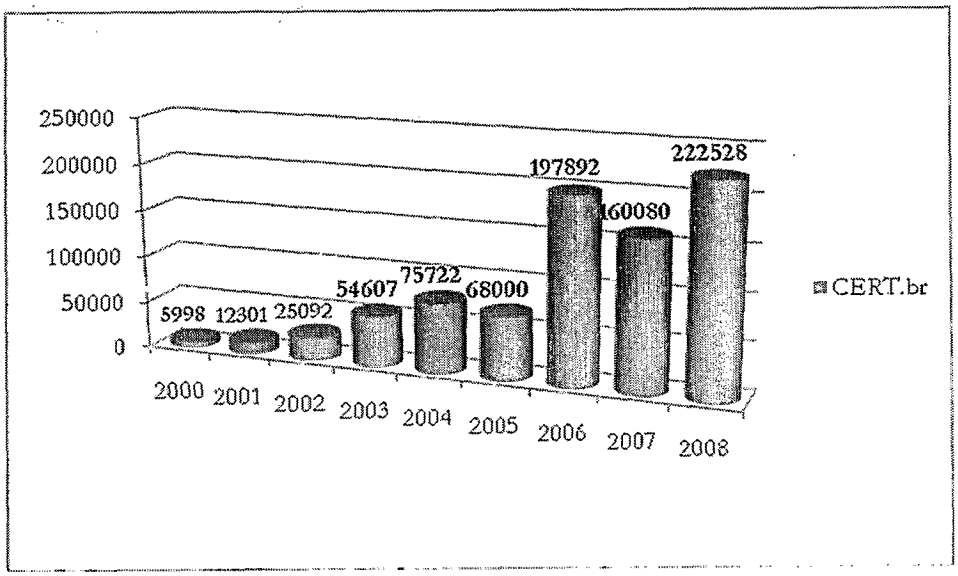
---

[۱] Evasion

[۲] Bypass



(الف)



(ب)

شکل ۱-۲ آمارهای رخدادهای امنیتی گزارش شده در (الف) MyCERT (ب) CERT.br

با توجه به نکات مطرح شدهٔ فوق، سیستم‌های تشخیص نفوذ می‌بایستی با کارایی مطلوب علاوه بر بازرسی[۱] حجم بالای اطلاعات، قادر به تشخیص رفتارهای ناهنجار از رفتارهای عادی مشاهده شده از منابع باشند. این نیازمندی‌ها در تبیین

---

۱ Inspection

معیارهای اصلی کیفیت و کارکرد سیستم‌های تشخیص نفوذ مورد استفاده قرار می‌گیرند. وجود معیارهای مناسب در این زمینه، سنجش و ارزیابی راه‌حل‌ها و معماری‌های پیشنهادی را ممکن می‌نماید. در نتیجه با توجه به مسیری که سیستم-های تشخیص نفوذ از ابتدای پیدایش تاکنون طی نموده‌اند و همچنین با پیش‌بینی فناوری‌های آتی، کارایی سیستم‌های تشخیص نفوذ با بررسی معیارهای مناسب مشخص خواهد شد. در ادامه جهت ارزیابی و سنجش سیستم‌های تشخیص نفوذ، معیارهای سرعت، صحت تشخیص و دقت تشخیص به عنوان مهمترین معیارهای در نظر گرفته شده در فرآیند تشخیص نفوذ مورد بررسی قرار می‌گیرد [4]:

۱. سرعت

از مهمترین معیارها برای فرآیند تشخیص نفوذ و در حالت کلی، برای بازرسی، نظارت[۱] و ممیزی[۲] سرعت پردازش می-باشد. بالا بودن سرعت تشخیص در یک سیستم تشخیص نفوذ بدین معنا است که سیستم تشخیص نفوذ قابلیت پردازش تمام اطلاعات ورودی را در مدت زمان مشخص دارا می‌باشد. همانطور که پیش از این اشاره شد، سرعت شبکه‌ها به صورت روز افزونی در حال افزایش است، بنابراین افزایش سرعت سیستم‌های تشخیص نفوذ در ارتباط با این مسئله ضروری می‌باشد. علاوه بر این، یکی از محدودیت‌هایی که باعث می‌شود سیستم‌های تشخیص نفوذ مبتنی بر شبکه به صورت گسترده در ستون اصلی[۳] اینترنت استفاده نشود، پایین بودن سرعت سیستم‌های تشخیص نفوذ برای پردازش بسته‌های عبوری است.

۲. صحت و دقت تشخیص

اشتباه مثبت و اشتباه منفی پارامترهای شناخته‌شده‌ای می‌باشند که تعیین‌کنندهٔ سطح صحت و دقت تشخیص در سیستم‌های تشخیص نفوذ می‌باشند. تشریح هر یک از این پارامترها در ادامه خواهد آمد:

---

[۱] Monitoring

[۲] Audit

[۳] Backbone

اشتباه مثبت[۱] رویدادی است که در آن، سیستم تشخیص نفوذ یک فعالیت درست و هنجار را به اشتباه یک حمله تشخیص می‌دهد. این پارامتر یک معیار بسیار مهم در تشخیص نفوذ می‌باشد. سیستم‌های تشخیص نفوذ به جهت جلوگیری از هشدارهای نادرست و رسیدن به حداقل اشتباه مثبت می‌بایستی مکانیزم‌های مناسبی را در فرآیند تشخیص نفوذ اتخاذ نمایند. در مقابل اشتباه منفی[۲] رویدادی است که در آن، سیستم تشخیص نفوذ در شناسایی یک حمله عاجز می‌ماند. این معیار نیز به مانند اشتباه مثبت، یک معیار مهم برای مقایسهٔ سیستم‌های تشخیص نفوذ می‌باشد. هر چه میزان اشتباه منفی در یک سیستم تشخیص نفوذ کمتر باشد، سیستم تشخیص نفوذ کارایی مناسب‌تری خواهد داشت.

افزایش کارایی سیستم‌های تشخیص نفوذ مورد توجه بسیاری از پژوهشگران قرار گرفته است. طراحی و پیاده‌سازی سخت‌افزاری بخش‌های حساس سیستم‌های تشخیص نفوذ از جمله ایده‌های مطرح شده برای بهبود کارکرد این سیستم-ها می‌باشد. در این زمینه تحقیقات بسیاری جهت بررسی مشکلات سیستم‌های تشخیص نفوذ و طراحی معماری‌های موثر برای کاهش این مشکلات ارائه شده است. بر این اساس و علاوه بر معیارهای اصلی، راه‌حل‌های ارائه شده برای پیاده‌سازی سخت‌افزاری سیستم‌های تشخیص نفوذ می‌بایست با توجه به معیارهای تاخیر، توان‌مصرفی و فضا امکان‌پذیر باشد. به علاوه، این راه‌حل‌ها می‌بایست با تغییر شرایط و افزایش و یا کاهش عواملی نظیر منابع تحت ممیزی[۳] و الگوهای[۴] تهاجمات مقیاس‌پذیر و انعطاف‌پذیر باشد.

گزارش پیش‌رو حاصل پژوهش انجام شده در این زمینه برای بهبود کارایی سیستم‌های تشخیص نفوذ مبتنی بر شبکه می‌باشد. برای این‌کار در فصل دوم از این گزارش، پژوهش‌های انجام شده مورد ارزیابی و دسته‌بندی قرار می‌گیرد. در این فصل علاوه بر بررسی معیارهای در نظرگرفته شده برای هریک از پژوهش‌های مرتبط پیشین و تحلیل نقاط ضعف و قوت آنها، یک طبقه‌بندی از شتاب‌دهنده‌های سخت‌افزاری برای معماری‌های سیستم‌های تشخیص نفوذ ارائه می‌گردد. فصل-های سوم و چهارم به تشریح معماری‌های پیشنهادی برای بخش‌های مبتنی بر سوءاستفاده و مبتنی بر ناهنجاری

---

[۱] False Positive

[۲] False Negative

[۳] Audit source

[۴] Rule

اختصاص دارد. روش‌های تشخیص، طراحی ساختارهای سخت‌افزاری مبتنی بر این روش‌ها و نحوهٔ شبیه‌سازی و ارزیابی روش‌ها و ساختارها به همراه نتایج ارزیابی برای هر یک از معماری‌های مبتنی بر سوء استفاده و مبتنی بر ناهنجاری، جزئیات فصول سوم و چهارم را تشکیل می‌دهد. در فصل پنجم بهبود مضاعف کارایی با بهره‌برداری ترکیبی از ساختارهای کارای معرفی شده در فصول قبل تشریح می‌گردد. جمع‌بندی نهایی آخرین فصل از این گزارش را تشکیل می‌دهد.

فصل ۲) طبقه‌بندی پژوهش‌های پیشین

در این فصل، پژوهش‌های پیشین که در زمینهٔ معماری‌های سخت‌افزاری سیستم‌های تشخیص نفوذ ارائه شده است، مورد تجزیه و تحلیل قرار می‌گیرد. برای این‌کار، معیارها و اولویت‌های این پژوهش‌ها در شناسایی و رفع مشکلات سیستم‌های تشخیص نفوذ بررسی می‌شود. در این پژوهش‌ها با تمرکز بر معیارهای لحاظ شده، بررسی گلوگاه پیشین و یا فعلی سیستم‌های تشخیص نفوذ، روش‌ها و ساختارهای مختلفی برای رفع و یا کاهش اثر آنها ارائه شده است. تحلیل مجموعهٔ دیدگاه‌ها بخش دیگری از این فصل را تشکیل خواهد داد.

نکته‌ای که می‌بایست در بررسی این پژوهش‌ها مورد توجه قرار گیرد، نیاز به ارائهٔ یک طبقه‌بندی جامع در زمینهٔ طراحی شتاب‌دهنده‌های سخت‌افزاری سیستم‌های تشخیص نفوذ شبکه و معماری‌های مربوط به آن احساس می‌شود. وجود یک دسته‌بندی مناسب از حوزه‌های پژوهشی انجام شده می‌تواند دیدگاه مناسبی را در شناسایی دقیق‌تر مزایا و معایب هر یک از حوزه‌ها و پژوهش‌های مرتبط با آن فراهم نماید. در این صورت، امکان تعریف حوزه‌های تحقیقاتی جدید و توسعهٔ معماری‌های با کارایی بیشتر در آن حوزه‌ها وجود خواهد داشت.

اگر چه طبقه‌بندی‌های معتبری برای سیستم‌های تشخیص نفوذ به صورت عمومی و با توجه به نوع منابع و ورودی سیستم[۱] (شامل سیستم‌های تشخیص نفوذ مبتنی بر میزبان[۲] و مبتنی بر شبکه[۳])، نوع و مکانیزم تشخیص (مبتنی بر سوءاستفاده[۴] و مبتنی بر ناهنجاری[۵]) و نحوهٔ پردازش این سیستم‌ها (سیستم‌های تشخیص نفوذ متمرکز[۶] و توزیع‌شده[۷]) وجود دارد، اما همچنان خلا وجود یک طبقه‌بندی مناسب برای انواع معماری‌ها و شتاب‌دهنده‌های سخت افزاری که در پروژه‌ها و پژوهش‌های مختلف در این حوزه پیشنهاد شده است، احساس می‌شود. با اینکه در برخی از این مطالب فنی،

---

[۱] Input Source

[۲] Host-based Intrusion Detection Systems

[۳] Network-based Intrusion Detection Systems

[۴] Misused-based

[۵] Anomaly-based

[۶] Centralized

[۷] Distributed

دسته‌بندی‌هایی با عنوان مرور بر معماری‌ها یا عناوین مشابه ارائه شده است، اما این دسته‌بندی‌ها بر اساس معیارهای دقیق صورت نگرفته است. در برخی از این دسته‌بندی‌ها تداخل[۱] قابل مشاهده است. بنابراین در بخش‌های آتی این فصل، علاوه بر بررسی پژوهش‌های معتبر پیشین، ارائهٔ یک طبقه‌بندی قائم[۲] برای شتاب‌دهنده‌های سخت‌افزاری در سیستم‌های تشخیص نفوذ مورد توجه قرار گرفته است.

در ادامه، پژوهش‌های پیشین از دو دیدگاه طبقه‌بندی خواهند شد. دیدگاه نخست، ساختارهای پیشنهادی بر اساس گلوگاه معرفی شده به همراه روش‌ها و طراحی‌های ارائه شده برای رفع آن می‌باشد. جزئیات مربوط به این طراحی‌ها و ساختارهای[۳] مبتنی بر آن در بخش ۲-۱ آمده است. دیدگاه دوم، بر اساس بسترهای[۴] پیشنهادی به جهت پیاده‌سازی راه‌حل‌های ارائه شده می‌باشد. دسته‌بندی بسترهای سخت‌افزاری نیز در بخش ۲-۲ ارائه شده است.

۲-۱- روش‌ها و ساختارها

این بخش به بررسی و تحلیل پژوهش‌ها و کارهای مرتبط از دیدگاه نوع طراحی و با توجه به گلوگاه شناسایی شده در آن‌ها اختصاص دارد. دسته‌بندی ارائه شده بخش نخست از طبقه‌بندی شتاب‌دهنده‌های سخت‌افزاری را برای سیستم‌های تشخیص نفوذ تشکیل می‌دهد. برای مجموعه مقالات و گزارش‌های فنی مورد ارجاع در این بخش، معیارهای در نظر گرفته شده برای بهبود عملکرد سیستم‌های تشخیص نفوذ بررسی شده و گلوگاه‌های فرض شده در سیستم‌های تشخیص نفوذ به عنوان دغدغه‌های اصلی نویسندگان هر یک از آن مقالات و گزارش‌های علمی فهرست می‌گردد. ساختار کلی راه-حل‌های ارائه شده و طراحی مبتنی بر آن بخش دیگری از بررسی مراجع را تشکیل می‌دهد. در نهایت برای هر یک و یا هر دسته از پژوهش‌ها نقاط قوت وضعف آن ارزیابی و تشریح می‌گردد. علاوه بر مطالب عنوان شده، طبقه‌بندی شتاب-

---

[۱] Conflict

[۲] Orthogonal

[۳] Structures

[۴] Platforms