دانشکده فنی

پایان‌نامه کارشناسی ارشد
رشته مهندسی کامپیوتر
گرایش نرم‌افزار

عنوان:

راهنمای نگارش پایان‌نامه و گزارش‌های علمی با ویرایش‌گر LaTeX

نگارش:

نام و نام خانوادگی دانشجو

اساتید راهنما:

نام و نام خانوادگی استاد راهنمای اول
نام و نام خانوادگی استاد راهنمای دوم

ماه و سال دفاع (مثلاً شهریور ۱۳۹۲)

دانشگاه گیلان
دانشکده فنی

پایان‌نامه کارشناسی ارشد

راهنمای نگارش پایان‌نامه و گزارش‌های علمی با ویرایش‌گر LaTeX

نگارش: نام و نام خانوادگی دانشجو

اساتید راهنما: نام و نام خانوادگی استاد راهنمای اول امضاء:

نام و نام خانوادگی استاد راهنمای دوم امضاء:

استاد ممتحن داخلی: دکتر ممتحن داخلی امضاء:

استاد ممتحن خارجی: دکتر ممتحن خارجی امضاء:

تاریخ:

تقدیم

اگر قابل تقدیم باشد تقدیم می‌دارم به:

تقدیر و تشکر

با سلام خدمت دانشجویان عزیز گروه مهندسی کامپیوتر دانشگاه گیلان:

مدت‌ها بود در این فکر بودم که با اندک تجربه‌ای که در آزمایشگاه امنیت داده و شبکه دانشگاه صنعتی شریف به‌دست آوردم، قالب استاندارد مناسبی را برای نگارش گزارش‌های علمی اعم از پایان‌نامه کارشناسی ارشد، پایان‌نامه کارشناسی، گزارش سمینار کارشناسی ارشد، گزارش کارآموزی دوره کارشناسی و به‌طور کلی هر گونه ارائه گزارشی فراهم نمایم. این قالب بر اساس بسته فارسی نرم‌افزار LaTeX یعنی $Xepersian$ توسعه داده شده است و استفاده از آن گرچه ابتدا کمی زمان‌بر است، ولی پس از آشنایی با دستورات این بسته درخواهید یافت که تهیه گزارش‌ها به چه میزان برای شما آسان و شیرین خواهد بود و دیگر دردسرهای نرم‌افزار تایپ MS_Word را نخواهید داشت.

به‌طور کلی استفاده از نرم‌افزار LaTeX نسبت به نرم‌افزارهای تایپی دیگر نظیر MS_Word برتری‌های بسیار محسوسی دارد. برای نمونه شما برای این‌که تفاوت بین این دو را دریابید، می‌توانید به آدرس $http://openwetware.org/wiki/Word_vs._LaTeX$ مراجعه نمایید. در این قالب سعی کرده‌ام تا تقریبا تمامی مواردی را که در نگارش یک پایان‌نامه و یا گزارش مناسب موردنیاز است را مدنظر قرار دهم و نمونه‌ای از کاربرد هر یک از دستورات را در قالب بیاورم که با آن آشنایی اولیه داشته باشید و سپس بر اساس نیازهای خود آن‌ها را تغییر دهید.

من به‌شخصه این قالب را با راهنمایی جناب آقای مهندس مؤمنی(نامزد دکتری آزمایشگاه امنیت داده و شبکه دانشگاه صنعتی شریف که جا دارد در این‌جا از ایشان تشکر نمایم) پی‌ریزی نموده‌ام و برای این منظور از پیشنهادات مناسب و ارزشمند جناب آقای دکتر شاه‌بهرامی، مدیریت گروه مهندسی کامپیوتر دانشگاه گیلان، بهره برده‌ام تا به‌نوبه خود قدم کوچکی را برای گروه مهندسی کامپیوتر دانشگاه گیلان در زمینه تهیه پایان‌نامه‌ها و گزارش‌های مناسب و دقیق برداشته باشم.

در ادامه برخی از مهم‌ترین ویژگی‌ها و مواردی را که در این قالب لحاظ کرده‌ام را، خدمت شما آورده‌ام. مهم‌ترین مواردی که در این قالب لحاظ شده است، عبارتند از:

- جلد اول پایان‌نامه و یا گزارش
- صفحه مربوط به امضای اساتید راهنما و ممتحن جهت ارزیابی پایان‌نامه یا گزارش
- لحاظ کردن صفحه چکیده فارسی
- لحاظ کردن فهرست مطالب تا ریزدانگی سه سطح با درج اتوماتیک
- لحاظ کردن فهرست شکل‌های پایان‌نامه یا گزارش تا ریزدانگی دو سطح
- لحاظ کردن فهرست جداول پایان‌نامه یا گزارش تا ریزدانگی دو سطح
- مدیریت فصل‌بندی
- مدیریت و درج مراجع
- مدیریت درج پاورقی‌ها با دو نوع امکان $reset\ per\ page$ و $reset\ per\ chapter$.

- نمایش یک فهرست اولیه از محتوای هر فصل در ابتدای هر فصل از پایان‌نامه و یا گزارش
- درج تصویر با هر فرمت و انواع جداول در سند
- درج شبه کد و یا الگوریتم در سند به همراه شماره الگوریتم و شماره فصل آن
- درج واژه‌نامه فارسی به انگلیسی از واژه‌های مهم به‌کار برده شده در سند
- لحاظ کردن صفحه چکیده انگلیسی
- جلد پایان‌نامه و یا گزارش به زبان لاتین

در ادامه نیز توضیحاتی را درباره خود نرم‌افزار LaTeXو طریقه کار با آن آورده‌ام.

LaTeXبه صورت پیش فرض در سیستم عامل لینوکس کار می کند، اما چندین $Distribution$ دارد که یکی از آنها $MikTex$ است و تمامی امکانات LaTeXدر محیط ویندوز را دارد. در صورتی که مایل هستید LaTeXکار کنید و نمی خواهید سیستم عامل ویندوز را ترک کنید از $MikTex$ استفاده کنید.

استفاده از $MikTex$ در محیط ویندوز امکاناتی به مراتب گسترده تر از LaTeXرا در اختیار شما قرار خواهد داد. این نرم افزار با استفاده از یک ادیتور جانبی که روی آن نصب می شود می تواند تجربه بسیار راحت تری در اختیار شما قرار دهد. این ادیتورها محیطی شبیه به ابزارهای برنامه نویسی پیشرفته که هنگام تایپ دستورات آن را کامل می کنند و پارامترهای مختلف را به شما پیشنهاد می دهند عمل کرده و سرعت و دقت و کارایی شما را تا حد قابل ملاحظه ای افزایش می دهد. یکی از این ادیتور ها که رایگان نیز میباشد نرم افزار $TeXnicCenter$ می باشد که از لینک زیر قابل دریافت است. این نرم افزار را پس از نصب $MikTex$ نصب کنید و در هنگام نصب زمانی که مسیر نصب LaTeXرا می خواهد مسیر محل نصب شده که حاوی فایل $latex.exe$ میباشد را به آن بدهید. (وقتی $MikTex$ هم نصب باشد همین مسیر است و فرقی ندارد)

$MikTex$ یکی از توزیع‌های مشهور Tex در ویندوز است.(به تازگی نسخهٔ لینوکس $MikTex$ نیز در حال ساخت است.) $MikTex$ مانند همهٔ توزیع‌های تک دارای چندین موتور حروف‌چینی، تعداد زیادی قلم، و تعداد بسیار زیادی بسته ($Package$) است. $MikTex$ رایگان است، هرچند که می‌توانید CD یا DVD آن را بخرید.

نسخهٔ کامل $MikTex$ دارای همهٔ بسته‌های موجود برای حروف‌چینی است. برای گرفتن این نسخه، نخست یک پروندهٔ کوچک با حجم حدود ۳ مگابایت را بارمی‌گیرید و سپس با اجرای آن، همهٔ بسته‌ها بارگرفته می‌شوند (حجم نسخهٔ کامل حدود ۹۰۰ مگابایت است). اگر این نسخه را داشته باشید، تقریباً هیچ‌گاه برای پردازش نوشته‌های خود به اینترنت نیازمند نخواهید بود (تنها ممکن است گاهی لازم شود که بسته‌های خود را به‌روزرسانی کنید).

نکتهٔ مهم: اگر می‌خواهید با $Xepersian$ نوشته‌های فارسی خود را بنویسید، نسخهٔ $MikTex$ شما باید ۲۰۷ یا بالاتر باشد. (بنابراین نسخهٔ $MikTex$ی که به همراه نرم‌افزار فارسی‌تک توزیع شده است، برای کار با $Xepersian$ مناسب نیست.

اگر نسخهٔ خلاصه یا نسخهٔ همراه $MikTex$ را بارگرفته باشید، بستهٔ $Xepersian$ هنوز در $MikTex$ شما نصب نشده است. بنابراین پس از نصب $MikTex$ باید این بسته‌ها را نیز به روشی که گفته خواهد شد به $MikTex$ خود بیفزایید. برای این کار، از منوی استارت ویندوز، به گزینهٔ $MikTex$ بروید و از آن‌جا

گزینهٔ *Packages Manager* را برگزینید (در نسخهٔ همراه، باید روی آیکون *MikTex* در *System Tray* کلیک‌راست کنید). با این کار، پنجره‌ای شامل فهرست همهٔ بسته‌های نصب‌شده و نصب‌نشدهٔ *MikTex* ظاهر خواهد شد. برای نصب *Xepersian* و *bidi* (و یا هر بستهٔ دیگر) کافی است نام آن بسته را (مثلاً *Xepersian*) در این فهرست بیابید و روی آن راست‌کلیک کنید و آن را برای نصب علامت بزنید. با این کار، *MikTex* خودش به اینترنت وصل خواهد شد و بستهٔ دلخواه شما را می‌گیرد و نصب می‌کند. حجم دو بستهٔ *Xepersian* و *bidi* کمتر از ۲ مگابایت است و بنابراین بارگیری آن چندان طول نخواهد کشید.

در ادامه چند نکته مهم را اشاره خواهیم کرد:

- برای رسیدن به نتیجهٔ درست حتماً باید آخرین نسخهٔ هر دو بستهٔ *Xepersian* و *bidi* را داشته باشید، وگرنه در پردازش خطا خواهید گرفت. توصیه می‌کنیم که بستهٔ *bidi* را (که در نسخهٔ همراه و خلاصه وجود دارد و ممکن است قدیمی شده باشد) حذف کنید و دوباره همزمان با *Xepersian* نصب کنید.

- اگر *Xepersian* و *bidi* را در این فهرست نیافتید، از منوهای این پنجره گزینهٔ *Synchronize* را بزنید تا فهرست نام‌های این پنجره به‌روز شود (برای این کار نیز دسترسی کوتاهی به اینترنت نیاز است).

- در صورتی که از نسخه ۲.۷ نرم افزار *MikTex* استفاده می کنید که از قبل داشته اید، این احتمال وجود دارد که برنامه به *Repository*های قدیمی تر متصل شود، برای اطمینان از این بابت از منوی *Repository* گزینه *Change Package Repository* را انتخاب کرده و یک منبع با نزدیک ترین زمان به روز رسانی را انتخاب کرده و سپس *Repository > Synchronize* را زده تا با منبع سنکرون شوید.

- ممکن است *MikTex* به صورت پیش فرض برای به روز رسانی بسته های *XeTeX* فعال نشده باشد. برای فعال کردن به روز کردن XeTeX از منوی *Start* به *MikTex > Settings* رفته و در نوار *Format* مطمئن شوید که جلوی *XeTeX* عبارت *Exclude* قرار نداشته باشد. سپس در نوار *General* کلید *Update Formats* را بزنید.

آخرین مطلب این که، اگر موردی احتیاج بود که نیاز بود در سند باشد و یا با مشکل مواجه شدید، به بنده با کانال ارتباطی *ali.a.r1368@gmail.com* اطلاع دهید تا اگر موردی بود ان‌شاالله برطرف گردد.

آرزوی توفیق و سلامتی برای همه شما

با احترام

علی احمدیان رمکی

چکیده

امروزه، روش‌های پیش‌گیری به‌تنهایی برای امنیت اطلاعات کافی نیستند. سیستم‌های هشدار زودهنگام در دسته روش‌های واکنشی در برابر تهدیدات امنیتی علیه سیستم‌ها و شبکه‌های کامپیوتری محسوب می‌شوند. این سیستم‌ها مکمل سیستم‌های تشخیص نفوذ هستند که هدف اصلی آن‌ها، تشخیص زودهنگام رفتارهای بالقوه مخرب در محیط‌های با مقیاس بزرگ نظیر سطوح ملی است. یکی از مهم‌ترین فرآیندها در سیستم‌های هشدار زودهنگام، تحلیل و همبسته‌سازی هشدارهای جمع‌آوری شده از حس‌گرهای نصب شده در شبکه تحت پوشش نظیر سیستم‌های تشخیص نفوذ، تلسکوپ‌های IP و سیستم‌های تشخیص کشف شبکه‌های بات است. در این پایان‌نامه، علاوه بر معرفی یک سیستم‌هشدار زودهنگام پیشنهادی برای تشخیص حملات اینترنتی، یک چارچوب کارا برای همبسته‌سازی هشدار در سامانه‌های هشدار زودهنگام پیشنهاد می‌گردد. این چارچوب پیشنهادی بر پایه ترکیبی از تکنیک‌های آماری و جریان‌کاوی عمل می‌نماید. این فرآیند به‌صورت بلادرنگ برای استخراج توالی رویدادهای بحرانی از دنباله هشدارها انجام می‌شود. توالی رویدادهای بحرانی می‌توایاند بخشی از یک سناریوی حمله چندمرحله‌ای باشند. علاوه بر این از یک ماتریس همبسته‌سازی هشدار نیز برای بیان میزان همبستگی بین نوع هشدارهای مختلف در یک سناریوی حمله چندمرحله‌ای، استفاده می‌شود. نتایج ارزیابی‌ها حاکی از آن است که چارچوب پیشنهادی به‌صورت کارا سناریوی حملات شناخته‌شده و حملات جدید ناشناخته را تشخیص می‌دهد. همچنین نتایج تجربی نشان می‌دهد که سیستم همبسته‌سازی هشدار پیشنهادی در شرایطی خاص تا حدود ۹۵% قادر به پیش‌گویی از گام‌های آتی مهاجم است.

کلمات کلیدی: امنیت شبکه، سامانه هشدار زودهنگام، همبسته‌سازی هشدار، حملات چندمرحله‌ای، طرح حمله.

فهرست مطالب

۱ مقدمه **۱**

۱.۱ ساختار پایان‌نامه ۵

۲ سامانه هشدار زودهنگام **۶**

۱.۲ اهمیت سیستم هشدار زودهنگام ۷

۲.۲ کاربردهای سیستم هشدار زودهنگام ۱۰

۱.۲.۲ پیشینه ۱۱

۳.۲ سیستم هشدار زودهنگام تعریف شده در امنیت اطلاعات ۱۱

۱.۳.۲ سیستم هشدار زودهنگام در مقابل IDS و IPS ۱۱

۴.۲ خلاصه فصل ۱۴

۳ همبسته‌سازی هشدار **۱۷**

۴ چارچوب همبسته‌سازی هشدار پیشنهادی **۱۹**

۵ پیاده‌سازی و ارزیابی **۲۰**

۶ جمع‌بندی و سوی کارهای آتی **۲۱**

مراجع **۲۴**

واژه‌نامهٔ فارسی به انگلیسی **۲۶**

فهرست شکل‌ها

۱.۲ اطلاعات مربوط به ۱۲ کشور بزرگ تولید کننده هرزنامه در سال ۲۰۱۲ [۱] ۹
۲.۲ سازمان کلی یک سیستم تشخیص نفوذ ۱۰
۳.۲ مراحل کلی عملکرد یک سیستم هشدار زودهنگام ۱۱
۴.۲ تفاوت‌های عملکردی سامانه هشدار زودهنگام در مقایسه با IDS و IPS الف) سیستم تشخیص نفوذ، ب) سیستم جلوگیری از نفوذ و ج) سیستم هشدار زودهنگام ۱۳

فهرست جدول‌ها

۱.۲ اطلاعات ده شبکه بزرگ بات بر اساس گزارش منتشر شده در سال ۲۰۱۲ [۲] ۸
۲.۲ مقایسه جنبه‌های مختلف سیستم هشدار زودهنگام با IDS و IPS ۱۵
۳.۲ مشخصات فنی و عملکردی سیستم‌های هشدار زودهنگام تجاری ۱۶

فصل ۱

مقدمه

امروزه سیستم‌های تشخیص نفوذ[۱] به‌طور قابل ملاحظه‌ای برای افزایش امنیت در سیستم‌های کامپیوتری مورد استفاده قرار می‌گیرند. تشخیص نفوذ فرآیند نظارت بر وقایع رخ‌داده در یک شبکه و یا سیستم کامپیوتری در جهت کشف موارد انحراف از سیاست‌های امنیتی است. هدف یک سیستم تشخیص نفوذ، جلوگیری از حمله نیست و تنها کشف و احتمالا شناسایی حملات و تشخیص اشکالات امنیتی در سیستم یا شبکه کامپیوتری و اعلان آن به مدیر سیستم است. بطور کلی IDS سه عملکرد اصلی نظارت، کشف و واکنش را بر عهده دارند. این سیستم‌ها در مواجهه با نقض سیاست‌های امنیتی، هشداری را جهت اعلان وضعیت جاری امنیتی، برای مدیران سطح بالا تولید می‌نمایند. به منظور مقابله با نفوذگران به سیستم‌ها و شبکه‌های کامپیوتری، روش‌های متعددی تحت عنوان روش‌های تشخیص نفوذ ایجاد گردیده است که عمل نظارت بر وقایع اتفاق افتاده در یک سیستم یا شبکه کامپیوتری را بر عهده دارد[۳].

اهمیت سیستم‌های تشخیص نفوذ در برقراری امنیت سیستم‌ها و شبکه‌های کامپیوتری، انکارناپذیر است. با وجود این، استفاده از سیستم‌های تشخیص نفوذ مشکلات مربوط به خود را داراست. این سیستم‌ها حجم زیادی از هشدارهای خام نفوذ را تولید می‌کنند که مدیریت این حجم از داده‌ها مسئله اصلی است. از جمله سایر ضعف‌هایی که می‌توان برای آن‌ها برشمرد عبارتند از:

- عدم توانایی لازم در بررسی حجم زیاد هشدارهای تولید شده
- بالا بودن میزان هشدارهای مثبت-غلط[۲]
- زمان‌بر بودن نگهداری دانش و به روز رسانی امضاها و الگو[۳]ها
- ناکارآمدی در کاربردهای بلادرنگ[۴]
- ناکارآمدی در تشخیص رخدادهای ناکامل که در آینده نزدیک، تبدیل به حملات واقعی خواهند شد.
- عدم کارایی آن‌ها در انتقال اطلاعات نفوذ به سایر مؤلّفه‌های امنیتی موجود در شبکه در یک مدت زمان کوتاه

[۱] Intrusion Detection Systems(IDSs)
[۲] False Positive
[۳] Pattern
[۴] Real Time

- ناکارآمدی برای تشخیص حملات ناشناخته

با وجود مشکلات ذکر شده برای سیستم‌های تشخیص نفوذ، محققان امنیت بر این باورند که همکاری سیستم‌های تشخیص نفوذ در یک محیط توزیع‌شده، سبب رفع و یا تقلیل برخی مشکلات ذکر شده خواهد شد[۴][۵]. این مفهومی است که سبب شکل‌گیری سیستم‌های تشخیص نفوذ همکار[۱] شده است. در این محیط‌ها، استفاده از مفهوم همبسته‌سازی هشدار[۲]ها، امری انکارناپذیر است. تحلیل‌گر همبسته‌ساز در محیط $CIDS$، بر اساس روابط منطقی بین هشدارها، هشدارها را گروه‌بندی می‌نماید. با توجه به همکاری سیستم‌های تشخیص نفوذ در محیط‌های همکار، کارایی و قدرت تشخیص تهدیدات، در این حالت به مراتب بیشتر از حالتی است که تنها از یک سیستم تشخیص نفوذ استفاده می‌شود.

از جمله چالش‌های موجود در این‌جا، چگونگی همبسته‌کردن هشدارهای خام دریافتی از حس‌گرهای متنوع و مدیریت نرخ مثبت-غلط است. انگیزه بکارگیری $CIDS$ها این است که هرIDS بر اساس الگوریتم تشخیص مختلفی پیاده‌سازی شده است و امضاهای مخصوص به خود را تولید می‌کند که ترکیب این IDSها می‌تواند یک تکنیک مناسب برای تشخیص دقیق و جامع‌تر باشد.

از جمله چالش‌های اصلی در بحث $CIDS$ها، میزان دقت، انعطاف‌پذیری، سازگاری با محیط‌های جدید، پیمانه‌ای بودن[۳] واحدهای تشخیص و همبسته‌ساز، توزیعی بودن و بلادرنگ بودن عملیات تشخیص است که تا حدودی بر روی آن‌ها مطالعاتی شده است اما به‌طور کامل محقق نشده است. از جمله ضعف‌های این سیستم‌ها عبارتند از:

- توصیف حملات معمولاً خیلی سطح پایین بوده و بنابراین تعیین و تفسیر آن‌ها دشوار است.
- برای هر حمله و هر نسخه تغییر یافته از الگوی حملات، نیاز به اضافه کردن یک الگوی جداگانه به پایگاه دانش است که این امر باعث بالا رفتن حجم پایگاه داده می‌گردد.
- هرچه الگوی حملات خاص‌تر باشد، نرخ مثبت-غلط کمتر خواهد شد. ولی اگر الگوی حملات خیلی خاص باشد، آنگاه مهاجم می‌تواند با ایجاد کمی تغییر در حمله مانع از کشف آن شود.

به‌نظر می‌رسد برای تشخیص سراسری تهدیدات اینترنتی در یک سطح وسیع، نیاز به یک عصر جدید در سیستم‌های کامپیوتری باشد، چیزی که باعث ظهور سیستم‌های هشدار زودهنگام شده است. متخصصان امنیت دریافته‌اند که راه‌حل‌های پیش‌گیرانه به‌تنهایی در مورد امنیت اطلاعات کافی نیست. بنابراین نیاز به روش‌های واکنشی است که حملات و تهدیدات را به موقع شناسایی کند. آن‌ها نیاز دارند به‌سرعت از تهدیدات بالقوه بر علیه شبکه‌ها و سیستم‌های خود مطلع شوند و آن تهدیدات را بر اساس میزان خطر الویت‌بندی کنند. اما تیم‌های امنیتی اغلب به ابزارهایی که اطلاعات مربوط به این تهدیدات را فراهم می‌کنند، دسترسی ندارند، معمولا زمانی به آن اطلاعات دسترسی پیدا می‌کنند که دیر شده است. این اطلاعات که با تأخیر دریافت می‌شوند، راه مؤثری برای کاهش تهدید فراهم نمی‌کنند و نمی‌توانند دید کلی از تهدید ایجاد کنند. چیزی که تیم‌های امنیتی نیاز دارند، یک راه‌حل هشدار زودهنگام[۴] است تا به آن‌ها در مدیریت تهدیدات[۵] کمک کند.

[۱] Co-operative Intrusion Detection Systems
[۲] Alert Correlation
[۳] Modularity
[۴] Early Warning Solution
[۵] Threats

سیستم‌های هشدار زودهنگام[۱] راهکاری واکنشی در مقابل تهدیدات امنیتی است. این سیستم‌ها مکمل سیستم‌های تشخیص نفوذ هستند که هدف اصلی آن‌ها تشخیص زودهنگام رفتارهای بالقوه سیستم، ارزیابی محدوده فعالیت‌های بدخواهانه[۲] و در نهایت نیز اعمال واکنش درخور در برابر هرگونه رخداد امنیتی قابل تشخیص است. سیستم‌های هشدار زودهنگام پس از سیستم‌های تشخیص نفوذ و سیستم‌های جلوگیری از نفوذ[۳]، افق جدیدی را برای امنیت اطلاعات و سامانه‌ها و شبکه‌های کامپیوتری ترسیم کرده‌اند. یک سیستم هشدار زودهنگام، رفتارهای ناشناخته‌ی سیستم را که به‌طور بالقوه مضر هستند شناسایی می‌کند، که شناسایی رفتارها بر اساس شاخص‌های اولیه انجام می‌شود.

سیستم‌های هشدار زودهنگام، نقش مهمی در به حداقل رساندن خسارات ناشی از حملات مختلف کامپیوتری دارند. این سیستم‌ها با بررسی رفتار کاربران یک سیستم یا یک شبکه کامپیوتری به دنبال نشانه‌های نفوذ می‌گردند و در صورت مشاهده‌ی رفتار خطرناک یا مشکوک مدیر سیستم را با دادن هشدار آگاه می‌سازند. همبستگی بین این علائم خام باعث فشرده‌سازی داده‌ها و کاهش داده‌های تکراری می‌شود.

هشدارهایی که حس‌گرهای تشخیص نفوذ یک سامانه هشدار زودهنگام تولید می‌کنند هشدارهای سطح پایینی هستند و چنانچه به‌صورت تک تک در نظر گرفته شوند، تهدیدات واقعی سیستم را به‌درستی نشان نمی‌دهند. معمولاً مهاجمین برای رسیدن به اهداف خود از حملات چند مرحله‌ای استفاده می‌کنند. به‌این صورت که در ابتدا از یک یا چند آسیب‌پذیری در سیستم استفاده کرده و حمله خود را یک گام جلو می‌برند و سپس با بهره‌گیری از پی‌آمدهای این گام که پیش‌نیاز گام بعدی حمله است، گام بعدی را اجرا می‌کنند و به این ترتیب حمله خود را گام‌به‌گام جلو می‌برند. حس‌گرهای تشخیص نفوذ سامانه هشدار زودهنگام، تنها قادر به تولید هشدارهای سطح پایین برای هر کدام از گام‌های حمله به‌صورت مجزا هستند و امکان تشخیص سناریوی حملات چندمرحله‌ای و ارتباط دادن هشدارهای یک حمله به یکدیگر را ندارند. بنابراین نیازمند ایجاد یک دید سطح بالاتر از وضعیت امنیتی سیستم هستیم. همبسته‌سازی هشدارها چنین تصویری را از سیستم و یا شبکه تحت حفاظت با پردازش بر روی هشدارهای حس‌گرهای تشخیص نفوذ در یک سامانه هشدار زودهنگام تولید می‌کند.

به‌طور کلی دو یا چند حس‌گر تشخیص نفوذ ممکن است برای اهداف زیر با یکدیگر همکاری کنند:

- تحلیل هشدارهای صادر شده یکدیگر
- تکمیل پوشش
- تقویت هشدارهای یکدیگر و پایین آوردن نرخ مثبت-غلط

همبسته‌سازی هشدارها فرآیندی است که طی آن هشدارهای تولید شده توسط یک یا چند حس‌گر موجود در شبکه، تحلیل می شود تا یک دیدگاه مختصر و سطح بالایی از تلاش‌های نفوذ احتمالی فراهم گردد. همبسته‌ساز با بررسی هشدارهای تولید شده و کشف ارتباطات منطقی آن‌ها به‌جای تولید صدها هشدار سطح پایین و گسسته، یک هشدار سطح بالا را به مدیر سیستم ارائه می‌کند[۶]. بنابراین تعیین رخدادهای بسیار مهم از میان حجم زیادی از وقایع ثبت شده، هدف نهایی فرآیند همبسته‌سازی است تا کیفیت هشدارها افزوده و تعداد آن‌ها کاسته

[۱] Early Warning Systems(EWS)
[۲] Malicious Activities
[۳] Intrusion Prevention System(IPS)

شود[۷]. علاوه بر حجم بالای هشدارها، می‌توان دلایل دیگری نیز برای اهمیت نیاز به همبسته‌سازی هشدارها برشمرد که عبارتند از:

۱. نرخ بالای هشدارهای مثبت-غلط

۲. ایجاد امکان همکاری بین حس‌گرهای تشخیص نفوذ

۳. ایجاد دید سطح بالاتری از رخدادهای بدخواهانه در شبکه برای مدیر امنیتی سیستم و کمک به تصمیم‌گیری درست و به‌موقع در مقابل حملات

۴. عدم تشخیص سناریوی حملات چندمرحله‌ای توسط حس‌گرهای تشخیص نفوذ ساده

تاکنون روش‌های زیادی برای همبسته‌سازی هشدار بیان شده است. مشکل اصلی بیشتر روش‌های همبسته‌سازی عدم کارایی آن‌ها برای کاربردهای بلادرنگ است. به‌دلیل اینکه در کاربردهای بلادرنگ نیازمند الگوریتم‌هایی با کارایی مناسب هستیم. برای مثال، در برخی از روش‌هایی که فرآیند همبسته‌ساری برای تشخیص سناریوی حملات چندمرحله‌ای به‌کار گرفته شده است، مرحله یادگیری دارای سربار زیادی است به‌گونه‌ای که کارایی سیستم تحت تأثیر این فرآیند قرار می گیرد. در این پایان‌نامه، ضمن معرفی یک سامانه هشدار زودهنگام پیشنهادی با نام $BEWS$، الگوریتم همبسته‌سازی مناسب و کارایی با نام $RTECA$ ارائه شده است که با یادگیری سناریوی حملات، هشدارهای زودهنگامی را که نشان‌دهنده گام‌های بعدی مهاجم در شبکه هدف است، تولید می‌نماید.

الگوریتم $RTECA$ بر اساس تصفیه توالی رویدادهای بحرانی که می‌توانند بخشی از سناریوی حملات چندمرحله‌ای باشند، عمل می‌نماید. چارچوب همبسته‌سازی پیشنهادی با استفاده از ترکیبی از روش‌های آماری و جریان‌کاوی در دو مود عملیاتی برخط و برون از خط کار می‌کند. در مود برخط با استفاده از ساخت یک درخت توالی رویداد به‌کمک ماتریس همبسته‌سازی هشدار، رفتارهای مهاجم را یاد می‌گیرد. در فاز برخط نیز با استفاده از هشدارهای دریافتی، سناریوی حملات شناخته شده را تشخیص داده و قوانین پیش‌گویی را تولید می‌نماید. علاوه بر این با استفاده از یک ماتریس همبسته‌سازی هشدار پویا، قادر به تشخیص سناریوی حملات جدید ناشناخته نیز خواهد بود. در ادامه با ارزیابی الگوریتم پیشنهادی بر روی مجموعه داده $DARPA$ 2000 با هدف تشخیص سناریوی حملات شناخته شده، مجموعه داده GCP با هدف سناریوی حملات جدید ناشناخته و یک مجموعه داده آزمایشگاهی جدید با نام $BISset$ با هدف تشخیص طرح حمله مهاجم، قادر به دستیابی به این اهداف با دقت قابل‌قبولی بوده‌ایم به‌طوری که ویژگی‌های زیر در این الگوریتم مدنظر قرار داده شده است:

۱. انجام تحلیل بلادرنگ هشدارهای نفوذ با استفاده از ترکیب تکنیک‌های جریان‌کاوی و آماری

۲. تطابق و تناسب الگوریتم با ماهیت جریان هشدارها

۳. ترکیب دانش قبلی در رابطه با همبستگی هشدارها و دانش آماری استخراج شده در حین اجرای الگوریتم

۴. کارایی قابل توجه روش مورد استفاده از نظر زمان اجرای پردازش هشدارها نسبت به پژوهش‌های پیشین

۵. پیش‌بینی گام‌های بعدی حمله در استخراج سناریوها

۱.۱ ساختار پایان‌نامه

ادامه این پایان‌نامه به‌صورت زیر سازماندهی شده است. در فصل ۲، ضمن بررسی اهمیت و جایگاه سامانه‌های هشدار زودهنگام پیشنهادی، به تشریح کامل مفهوم سامانه هشدار زودهنگام می‌پردازیم و پژوهش‌های صورت گرفته در این زمینه را دسته‌بندی خواهیم نمود. فصل ۳، به بررسی کارهای مرتبط در زمینه همبسته‌سازی هشدارها می‌پردازیم. در این فصل کارهای انجام شده در رابطه با همبسته‌سازی هشدارها را طبقه‌بندی نموده و مهم‌ترین کارهای صورت گرفته در هر طبقه را به‌طور مختصر معرفی کرده‌ایم. در فصل ۴، به معرفی همه‌جانبه سیستم هشدار زودهنگام پیشنهادی با نام $BEWS$ و چارچوب همبسته‌سازی هشدار ارائه‌شده مورد استفاده در آن با نام $RTECA$ با هدف کشف سناریوی حملات چندمرحله‌ای خواهیم پرداخت. فصل ۵ به ارزیابی تجربی الگوریتم با استفاده از سه مجموعه داده $DARPA2000$، GCP و $BISset$ و تحلیل جنبه‌های الگوریتم می‌پردازیم. در انتها، فصل ۶ نیز به جمع‌بندی و سوی کارهای آتی اختصاص دارد.

فصل ۲

سامانه هشدار زودهنگام

مطالب این فصل

۱.۲ اهمیت سیستم هشدار زودهنگام ۷
۲.۲ کاربردهای سیستم هشدار زودهنگام ۱۰
۱.۲.۲ پیشینه ۱۱
۳.۲ سیستم هشدار زودهنگام تعریف شده در امنیت اطلاعات ۱۱
۱.۳.۲ سیستم هشدار زودهنگام در مقابل IDS و IPS ۱۱
۴.۲ خلاصه فصل ۱۴

امروزه این نتیجه حاصل شده است که راه‌حل‌های پیش‌گیرانه به‌تنهایی در مورد امنیت اطلاعات کافی نیست. بنابراین نیاز به روش‌های واکنشی است که حملات و تهدیدات را به موقع شناسایی کند. متخصصان امنیت نیاز دارند به‌سرعت از تهدیدات بالقوه بر علیه شبکه‌ها و سیستم‌های خود مطلع شوند و آن تهدیدات را بر اساس میزان خطر الویت‌بندی کنند. اما تیم‌های امنیتی اغلب به ابزارهایی که اطلاعات مربوط به این تهدیدات را فراهم می‌کنند، دسترسی ندارند، معمولا زمانی به آن اطلاعات دسترسی پیدا می‌کنند که دیر شده است. این اطلاعات که با تأخیر دریافت می‌شوند، راه مؤثری برای کاهش تهدید فراهم نمی‌کنند و نمی‌توانند دید کلی از تهدید ایجاد کنند. چیزی که تیم‌های امنیتی نیاز دارند، یک راه‌حل هشدار زودهنگام است تا به آن‌ها در مدیریت تهدیدات کمک کند. سیستم‌های هشدار زودهنگام راهکاری واکنشی در مقابل تهدیدات امنیتی است. در این فصل به بیان اهمیت سامانه‌های هشدار زودهنگام در امنیت شبکه‌ها و سیستم‌های کامپیوتری خواهیم پرداخت. علاوه بر آن مهم‌ترین کاربردهای این سامانه‌ها را ذکر خواهیم کرد. در ادامه به تعریف دقیق این سامانه و تشریح ابعاد گوناگون از قبیل مهم‌ترین معماری‌ها و نیازمندی‌ها خواهیم پرداخت. سپس سیستم‌های هشدار زودهنگام موجود را در دو رده تحقیقاتی و عملیاتی بررسی خواهیم کرد و ضمن مرور اهداف هر یک از آن‌ها به تشریح جزئیات هر یک خواهیم پرداخت.

۱.۲ اهمیت سیستم هشدار زودهنگام

در طول دهه‌های گذشته، اینترنت و سیستم‌های کامپیوتری، کاربردهای فراوانی داشته‌اند که این افزایش استفاده، موضوعات امنیتی زیادی را بوجود آورده است. اساس امنیت سیستم‌ها و شبکه‌های کامپیوتری، بر سه اصل محرمانگی[۱]، جامعیت[۲] و دسترس‌پذیری[۳] است. سازمان‌های مختلف با داده‌های حساس، بر اساس سیاست‌های امنیتی مختلفی، هر یک به‌گونه‌ای خاص در جهت برآورده کردن این سه اصل اساسی امنیت تلاش می‌کنند. هرگونه فعالیت مخربانه توسط بدافزارها و حملات اینترنتی درصدد تخطی از این سه اصل هستند. گزارشات منتشر شده در سایت‌های $CERT$[۴] کشورهای مختلف و نیز شرکت‌هایی که بر روی امنیت شبکه و یا امنیت نرم‌افزار فعالیت می‌کنند، حاکی از این مسئله مهم است که این تهدیدات اینترنتی روز به‌روز در حال افزایش است.

بر اساس گزارشی از جیمز[۵] [۸]، تحقیقات نشان می‌دهد که در حال حاضر میزان تهدیدات اینترنتی برای ضربه زدن به شهرت افراد و یا بیان عقاید مهاجمان، به‌مراتب بیشتر از تهدیداتی است که جنبه مالی در آن‌ها هدف اصلی بوده است. طیف گسترده‌ای از تهدیدات اینترنتی برای رسیدن به مقاصد مهاجمان وجود دارد که از جمله مهم‌ترین آن‌ها انتشار ویروس‌ها، کرم‌ها، بدافزارهای مخرب، حملات منع سرویس و هرزنامه[۶]ها است. برای مثال، یکی از روش‌های حملات منع سرویس، ایجاد شبکه‌های بات[۷] است که سیلوا[۸] و همکارانش[۹] به خوبی ابعاد آن را تشریح کرده و موضوعات باز بر روی آن را بیان کرده است.

موسسه $Sophos$[۲] نیز گزارش جامعی از بکارگیری شبکه‌های بات که برای یک هدف مهم در سطح وسیعی بکارگرفته می‌شوند، آورده است. بر اساس این گزارش، ده شبکه بات بزرگ تا سال ۲۰۱۱ ، در جدول ۱.۲ آورده شده است. در این گزارش چاپ شده، به‌عنوان مثالی دیگر از کاربردهای شبکه بات، می‌توان به گسترش هرزنامه‌های اینترنتی اشاره کرد که تا سال ۲۰۱۲، میزان بیشترین تولید آن‌ها برای ۱۲ کشور دنیا در شکل ۱.۲ نمایش داده شده است. بر طبق یک گزارش دیگر از شرکت سیمنتک [۱] که در سال ۲۰۱۲ منتشر شد، میزان حملات مخرب بلاک‌شده توسط این شرکت در سال ۲۰۱۱، بیش از ۵۰۵ بیلیون بوده است که این میزان در مقایسه با سال قبل، ۸۱% افزایش داشته است.

اهمیت سیستم‌های تشخیص نفوذ در برقراری امنیت سیستم‌ها و شبکه‌های کامپیوتری، انکارناپذیر است. با وجود این، استفاده از سیستم‌های تشخیص نفوذ مشکلات مربوط به خود را داراست. این سیستم‌ها حجم زیادی از هشدارهای خام نفوذ را تولید می‌کنند که مدیریت این حجم از داده‌ها مسئله اصلی است. از جمله سایر ضعف‌هایی که می‌توان برای آن‌ها برشمرد عبارتند از:

- عدم توانایی در بررسی حجم زیاد هشدارهای تولید شده
- بالا بودن میزان هشدارهای مثبت-غلط

[۱] Confidentiality
[۲] Integrity
[۳] Availability
[۴] Computer Emeregency Response Team
[۵] James
[۶] Spam
[۷] Botnet
[۸] Silva

جدول ۱.۲: اطلاعات ده شبکه بزرگ بات بر اساس گزارش منتشر شده در سال ۲۰۱۲ [۲]

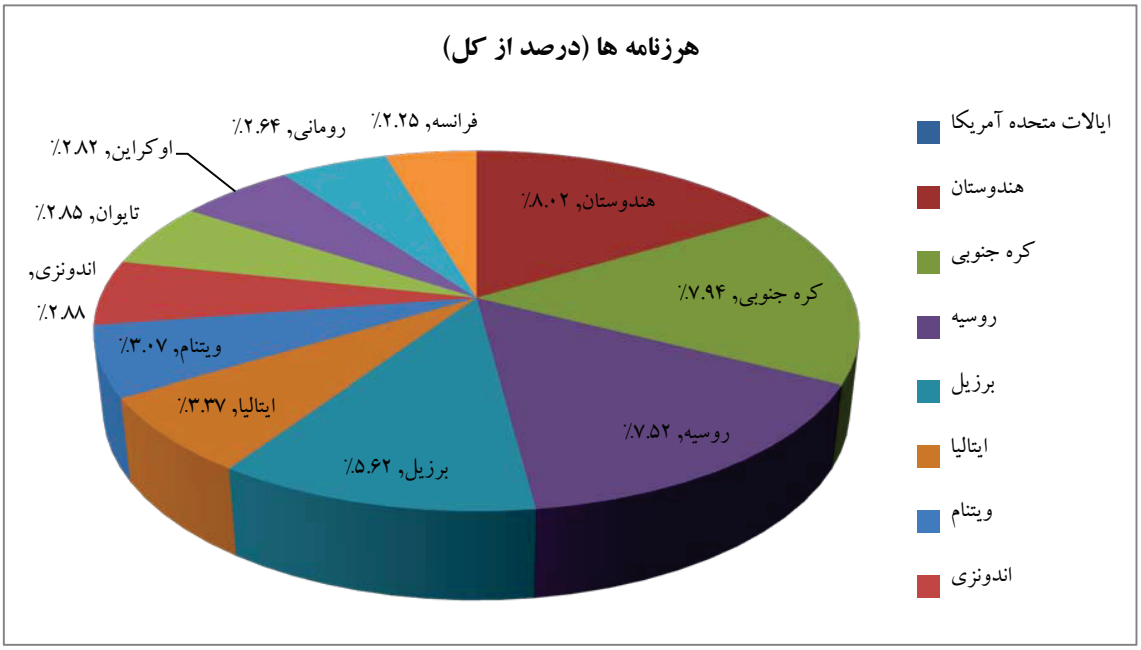
ردیف	نام عملگر شبکه بات	میزان قربانی	شهرت
۱	OneStreetTroop	٪۹/۳	Operator SpyEye
۲	RudeWarlockMob	٪۹	Gang TDL/TDSS
۳	FreakySpiderCartel	٪۷	Operator AV Rogue
۴	WhiteGloveGang	٪۶/۲	Operator Neosploit
۵	FiveLakeTrippers	٪۴/۵	Operator AV Rogue
۶	WildLightPosse	٪۲/۹	Operator Gbot
۷	SouthSideRiders	٪۲/۹	Operator AV Rogue
۸	TenPrisonMagicias	٪۲/۷	Operator Zeus
۹	GreedySideBoys	٪۲/۶	Operator Virut
۱۰	SmallRockNerds	٪۲/۱	Gang Downloader Eleonore

- زمان‌بر بودن نگهداری دانش و به روز رسانی امضاها و الگو
- ناکارآمدی در کاربردهای بلادرنگ
- ناکارآمدی در تشخیص رخدادهای ناکامل که در آینده نزدیک، تبدیل به حملات واقعی خواهند شد.
- عدم کارایی آن‌ها در انتقال اطلاعات نفوذ به سایر مؤلّفه‌های امنیتی موجود در شبکه در یک مدت زمان کوتاه
- ناکارآمدی برای تشخیص حملات ناشناخته

با وجود مشکلات ذکر شده برای سیستم‌های تشخیص نفوذ، محققان امنیت بر این باورند که همکاری سیستم‌های تشخیص نفوذ در یک محیط توزیع‌شده، سبب رفع و یا تقلیل برخی مشکلات ذکر شده خواهد شد[۴][۵]. این مفهومی است که سبب شکل‌گیری سیستم‌های تشخیص نفوذ همکار شده است. در این محیط‌ها، استفاده از مفهوم همبسته‌سازی هشدارها، امری انکارناپذیر است. تحلیل‌گر همبسته‌ساز در محیط $CIDS$، بر اساس روابط منطقی بین هشدارها، هشدارها را گروه‌بندی می‌نماید. با توجه به همکاری سیستم‌های تشخیص نفوذ در محیط‌های همکار، کارایی و قدرت تشخیص تهدیدات، در این حالت به مراتب بیشتر از حالتی است که تنها از یک سیستم تشخیص نفوذ استفاده می‌شود.

از جمله چالش‌های اصلی در بحث $CIDS$ها، میزان دقت، انعطاف‌پذیری، سازگاری با محیط‌های جدید، پیمانه‌ای بودن واحدهای تشخیص و همبسته‌ساز، توزیعی بودن و بلادرنگ بودن عملیات تشخیص است که تا حدودی بر روی آن‌ها مطالعاتی شده است اما به‌طور کامل محقق نشده است. به‌نظر می‌رسد برای تشخیص سراسری تهدیدات اینترنتی در یک سطح وسیع، نیاز به یک عصر جدید در سیستم‌های کامپیوتری باشد، چیزی که باعث ظهور سیستم‌های هشدار زودهنگام شده است.

امروزه این نتیجه حاصل شده است که راه‌حل‌های پیش‌گیرانه به‌تنهایی در مورد امنیت اطلاعات کافی نیست. بنابراین نیاز به روش‌های واکنشی است که حملات و تهدیدات را به موقع شناسایی کند. متخصصان امنیت نیاز



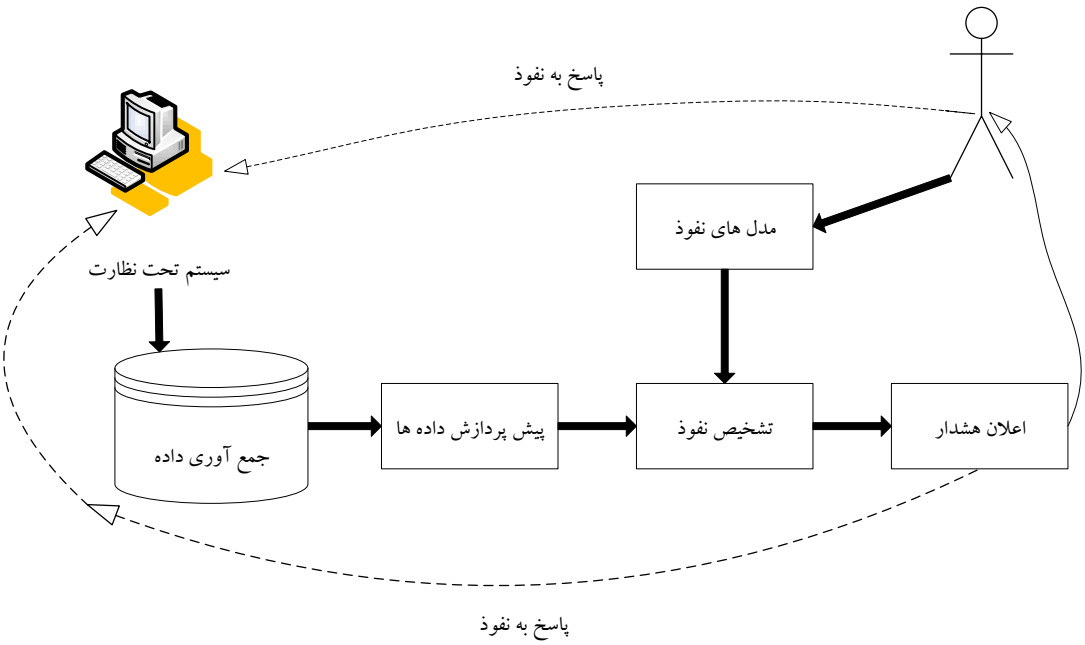
شکل ۱.۲: اطلاعات مربوط به ۱۲ کشور بزرگ تولید کننده هرزنامه در سال ۲۰۱۲ [۱]

دارند به‌سرعت از تهدیدات بالقوه بر علیه شبکه‌ها و سیستم‌های خود مطلع شوند و آن تهدیدات را بر اساس میزان خطر الویت‌بندی کنند. اما تیم‌های امنیتی اغلب به ابزارهایی که اطلاعات مربوط به این تهدیدات را فراهم می‌کنند، دسترسی ندارند، معمولا زمانی به آن اطلاعات دسترسی پیدا می‌کنند که دیر شده است. این اطلاعات که با تأخیر دریافت می‌شوند، راه مؤثری برای کاهش تهدید فراهم نمی‌کنند و نمی‌توانند دید کلی از تهدید ایجاد کنند. چیزی که تیم‌های امنیتی نیاز دارند، یک راه‌حل هشدار زودهنگام است تا به آن‌ها در مدیریت تهدیدات کمک کند.

سیستم‌های هشدار زودهنگام راهکاری واکنشی در مقابل تهدیدات امنیتی است. این سیستم‌ها مکمل سیستم‌های تشخیص نفوذ هستند که هدف اصلی آن‌ها تشخیص زودهنگام رفتارهای بالقوه سیستم، ارزیابی محدوده فعالیت‌های بدخواهانه و در نهایت نیز اعمال واکنش درخور در برابر هرگونه رخداد امنیتی قابل تشخیص است. سیستم‌های هشدار زودهنگام پس از سیستم‌های تشخیص نفوذ و سیستم‌های جلوگیری از نفوذ، افق جدیدی را برای امنیت اطلاعات و سامانه‌ها و شبکه‌های کامپیوتری ترسیم کرده‌اند. یک سیستم هشدار زودهنگام به‌عوان مکمل سیستم‌های تشخیص نفوذ، رفتارهای ناشناخته‌ی سیستم را که به‌طور بالقوه مضر هستند شناسایی می‌کند، که شناسایی رفتارها بر اساس شاخص‌های اولیه انجام می‌شود.

سیستم‌های هشدار زودهنگام، نقش مهمی در به حداقل رساندن خسارات ناشی از حملات مختلف کامپیوتری دارند. این سیستم‌ها با بررسی رفتار کاربران یک سیستم یا یک شبکه کامپیوتری به دنبال نشانه‌های نفوذ می‌گردند و در صورت مشاهده‌ی رفتار خطرناک یا مشکوک مدیر سیستم را با دادن هشدار آگاه می‌سازند. همبستگی بین این علائم خام باعث فشرده‌سازی داده‌ها و کاهش داده‌های تکراری می‌شود.

همبسته‌سازی هشدارها فرآیندی است که طی آن هشدارهای تولید شده توسط یک یا چند حس‌گر موجود در شبکه، تحلیل می شود تا یک دیدگاه مختصر و سطح بالایی از تلاش‌های نفوذ احتمالی فراهم گردد. همبسته‌ساز با بررسی هشدارهای تولید شده و کشف ارتباطات منطقی آن‌ها به‌جای تولید صدها هشدار سطح پایین و گسسته، یک هشدار سطح بالا را به مدیر سیستم ارائه می‌کند[۶]. بنابراین تعیین رخدادهای بسیار مهم از میان حجم



شکل ۲.۲: سازمان کلی یک سیستم تشخیص نفوذ

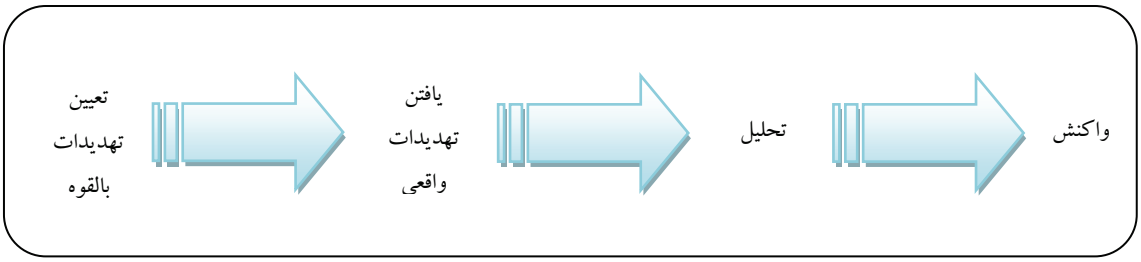
زیادی از وقایع ثبت شده، هدف نهایی فرآیند همبسته‌سازی است تا کیفیت هشدارها افزوده و تعداد آن‌ها کاسته شود[۷]. در فصل سوم، چارچوب اصلی همبسته‌سازی بیان می‌گردد.

۲.۲ کاربردهای سیستم هشدار زودهنگام

سیستم‌های هشدار زودهنگام، کاربردهای مختلفی دارند که در این قسمت قصد داریم، به مهم‌ترین کاربردهای آن اشاره کرده و برای هر کدام از دسته‌ها، مهم‌ترین نتایج تحقیقاتی و سیستم‌های عملیاتی را بیان کنیم. با توجه به طبیعت سیستم‌های هشدار زودهنگام و عملکرد پیش‌بینانه آن، تقریبا در تمامی کاربردهایی که انسان، اطلاعات و به‌طور کلی هر چیز مهمی را تهدید می‌کند، استفاده از این سیستم‌ها روش بسیار مناسبی است. با پیش‌بینی تهدیدات توسط این سیستم‌ها، تخریب ناشی از خطرات به کمترین حد ممکن کاهش می‌یابد. بکارگیری این سیستم‌ها در عرصه‌های مختلف تقریبا از سال ۲۰۰۰ به بعد، صورت گرفت.

در تمامی کاربردها، سیستم هشدار زودهنگام مبتنی بر چهار مرحله کلیدی مهم است که در شکل ۳.۲ آورده شده است[۱۰]. با ترکیب این چهار مؤلّفه و بکارگیری آن‌ها بر روی داده‌های خام ذخیره شده توسط حس‌گرهای سیستم‌های EWS حملات[۱] احتمالی کشف شده و قبل از تبدیل شدن به حملات واقعی[۲]، پیش‌بینی می‌گردند. هر کدام از این مؤلّفه‌ها در محیط عملیاتی توزیع شده‌اند. برای برخی کاربردها این مؤلّفه‌ها خاصیت استفاده مجدد دارند و برای سایر مؤلّفه‌ها می‌توان، برای کاربردهای خاص، جایگزین‌های مناسب را درنظر گرفت.

[۱] Potential Attacks
[۲] Actual Attacks



شکل ۳.۲: مراحل کلی عملکرد یک سیستم هشدار زودهنگام

۱.۲.۲ پیشینه

پیدایش سیستم هشدار زودهنگام، در دو دهه اخیر در کشور آمریکا بوده است. جایی که محققان این کشور بدنبال روش‌هایی برای پیش‌بینی خطرات طبیعی نظیر سیل، زلزله، آتش‌سوزی و غیره بوده‌اند. آن‌ها معتقد بودند که با هجوم انسان به منابع طبیعی و جنگل‌ها، اکوسیستم طبیعی موجود در جنگل تحت تأثیر رفتار آن‌ها قرار گرفته است و نسبت به تغییرات مقاوم نیستند. به این دلیل برخی از پژوهشگران مؤسسه $USDAForestService$ با همکاری $FederalState$ در صدد چاره‌ای برای جلوگیری از این تغییرات ناگهانی در اکوسیستم طبیعت بوده‌اند تا سلامت جنگل‌ها تضمین گردد. تلاش آن‌ها منجر به پیدایش ایده سیستم هشدار زودهنگام شد. این سیستم‌ها اطلاعات مبتنی بر تغییرات محیطی را ضبط کرده و تحلیل‌های لازم را انجام می‌دادند. $HFRA$[۱] یک پاسخ مناسب و زودهنگام برای این خواسته یافت[۱۱].

فرآیندهای کلیدی در تشخیص زودهنگام و واکنش مناسب در برابر تهدیدات محیطی، مرتبط کردن و طبقه‌بندی هشدارهای رسیده بود. این نخستین بار بود که تهدیدات محیطی با استفاده از چنین سیستم‌های پیش‌بینی شده و از آسیب‌های آن جلوگیری به‌عمل می‌آمد. در حقیقت عامل اصلی در موفقیت این سیستم‌ها پیش‌بینی به‌موقع تهدیدات احتمالی بود. پس از عملیاتی شدن این سیستم و به‌کارگیری آن در محیط واقعی، سیستم هشدار زودهنگام وارد عرصه جدیدی شد. با توجه به مطالعات صورت گرفته، به‌طور کلی سیستم هشدار زودهنگام در ۶ دسته مهم زیر کاربرد دارند. در ادامه ضمن بیان هر دسته، کارایی سیستم‌های هشدار زودهنگام در این دسته و مهم‌ترین کارهای صورت گرفته در هر دسته را شرح خواهیم داد.

۳.۲ سیستم هشدار زودهنگام تعریف شده در امنیت اطلاعات

در بخش قبل مهم‌ترین کاربردهای سیستم هشدار زودهنگام را بیان کردیم. در این بخش، جنبه‌های سیستم هشدار زودهنگام در بستر شبکه‌های بزرگ را با جزئیات بیشتر شرح خواهیم داد.

۱.۳.۲ سیستم هشدار زودهنگام در مقابل IDS و IPS

تشخیص نفوذ فرآیندی است که وقایع رخ داده شده در یک سیستم و شبکه کامپیوتری را نظارت می‌کند و نشانه‌های نفوذ را تحلیل می‌کند. در واقع هدف اصلی آن تشخیص رخ‌دادهای امنیتی است که نقض سیاست‌های

[۱] Healthy Forest Restoration Act

امنیتی تعریف شده توسط مدیر سیستم رادر پی دارد. امروزه، استفاده از سیستم‌های تشخیص نفوذ جهت برقراری امنیت، امری ضروری است. شکل ۴.۲، عملکرد هر یک از سیستم‌های تشخیص نفوذ، جلوگیری از نفوذ و هشدار زودهنگام را مورد مقایسه قرار می‌دهد. در جدول ۲.۲ این سه سیستم از جنبه‌های مختلف با یکدیگر مقایسه شده‌اند.

به‌طور کلی سیستم‌های تشخیص نفوذ از سه متدلوژی تشخیص مبتنی بر امضاء، مبتنی بر ناهنجاری و تحلیل حالت‌مند پروتکل [۳] استفاده می‌کنند که روش اول نیازمند یک پایگاه دانش از قبل تعریف‌شده حاوی امضاهای نفوذ است. در روش دوم رفتارعادی یک کاربر، به‌عنوان یک الگو ذخیره شده و حالت‌های خارج از این الگوها، به‌عنوان نفوذ تشخیص داده می‌شود. در روش سوم نیز با ردیابی حالت‌های پروتکل اتصال، فرمان‌ها و دنباله‌های غیرقابل انتظار را تشخیص می‌دهد. هر کدام از این روش‌ها دارای مزایا و معایبی هستند که توسط لیائو و همکارانش[۳] تشریح شده است. شیوه‌های تشخیص نفوذ توسط این سیستم‌ها نیز به پنج دسته کلی زیر تقسیم می‌شوند:

۱. **مبتنی بر آمار**[۱]: با استفاده از یک آستانه از پیش تعریف‌شده و به‌کارگیری احتمالات، نفوذ را تشخیص می‌دهد.

۲. **مبتنی بر الگو**[۲]: با استفاده از تطبیق الگوی حمله با رفتار مشاهده شده، نفوذ را تشخیص می‌دهد.

۳. **مبتنی بر قانون**[۳]: با استفاده از قوانین $If - Then$ و $Else\ If - Then$ یک مدلی را برای کاربر تعریف کرده و رفتار مشاهده‌شده را با این مدل مقایسه می‌کند. در صورت تخطی از این قوانین، نفوذ را تشخیص می‌دهد.

۴. **مبتنی بر حالت**[۴]: در این حالت برای حملات یک ماشین حالت متناهی ساخته می‌شود که در صورت مطابقت رفتار مشاهده شده با این ماشین، نفوذ تشخیص داده می‌شود.

۵. **مبتنی بر اکتشاف**[۵]: در این روش نیز با استفاده از مفاهیم بیولوژیکی و روش‌های هوش مصنوعی، نفوذ تشخیص داده می‌شود.

سیستم‌های تشخیص نفوذ از نظر روش‌های تشخیص نیز به پنج دسته اصلی زیر تقسیم می‌شوند[۳]:

۱. **مبتنی بر برنامه کاربردی**[۶]: کوچکترین سطح تعریف‌شده برای IDS بوده و رفتارهای یک برنامه کاربردی خاص را نظارت می‌کند.

۲. **مبتنی بر میزبان**[۷]: مشخصه‌های رفتاری میزبانان دارای اطلاعات حساس را جمع‌آوری و تحلیل می‌کند.

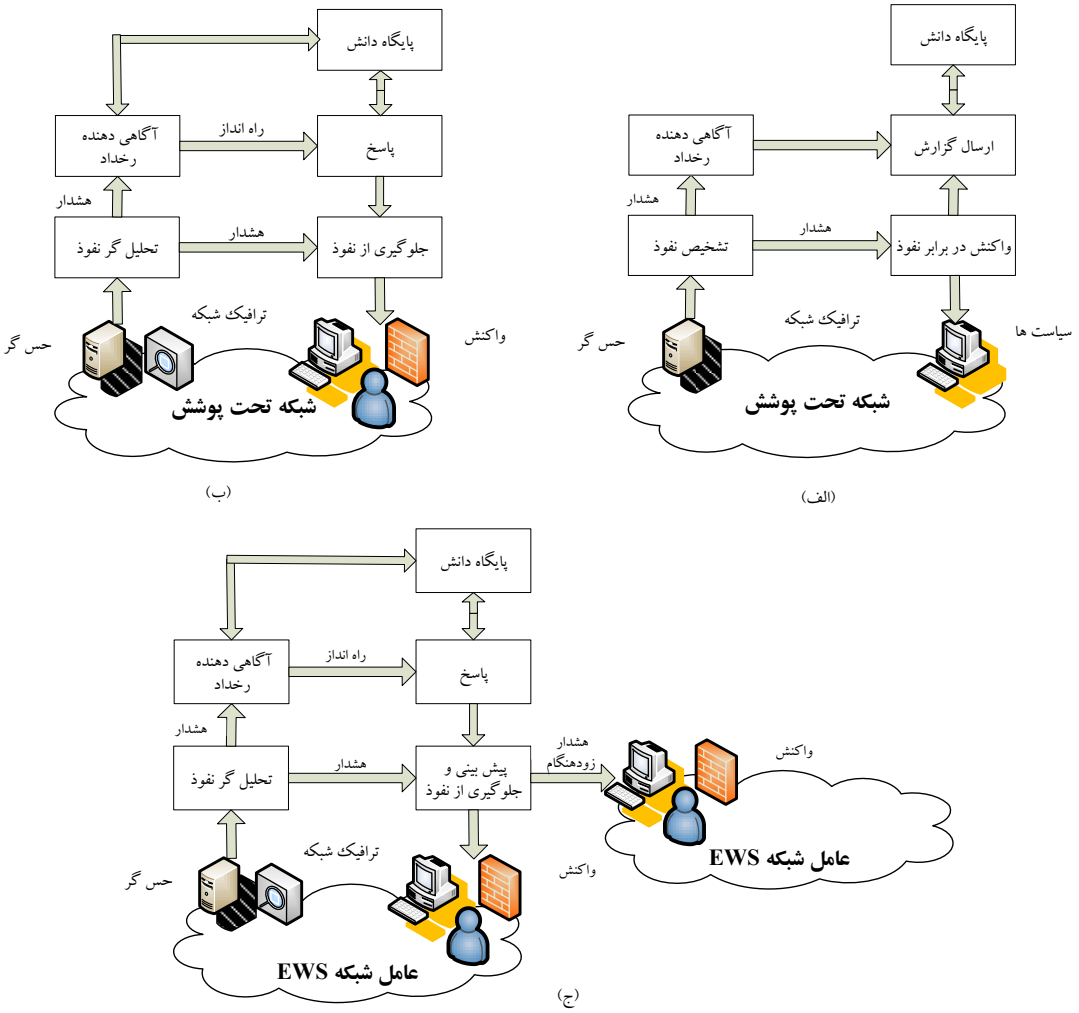
۳. **مبتنی بر شبکه**[۸]: ترافیک شبکه را دریافت کرده و رفتارهای مشکوک را تشخیص می‌دهد.

---

۱ Statistical-based
۲ Pattern-based
۳ Rule-based
۴ State-based
۵ Heuristic-based
۶ Application-based IDS (AIDS)
۷ Host-based IDS (HIDS)
۸ Network-based IDS(NIDS)

۴. **مبتنی بر ارتباطات بی‌سیم**[۱]: مانند سیستم مبتنی بر شبکه است با این تفاوت که در محیط‌های بی سیم به‌کار گرفته می‌شود.

۵. **تحلیل رفتار شبکه**[۲]: ترافیک شبکه را بررسی کرده و تا حملات را با استفاده از جریان شبکه غیرقابل انتظار تشخیص دهد.



شکل ۴.۲: تفاوت‌های عملکردی سامانه هشدار زودهنگام در مقایسه با IDS و IPS الف) سیستم تشخیص نفوذ، ب) سیستم جلوگیری از نفوذ و ج) سیستم هشدار زودهنگام

یکی دیگر از مفاهیم نوظهور جهت مقابله با تهدیدات اینترنتی، سیستم پیش‌گیری از نفوذ است. IPS ترکیبی از $NIDS$ و دیواره آتش است[۱۲]. IPS به‌کمک $NIDS$ سرآیند[۳] و پایه‌بار[۴] بسته‌های اطلاعاتی را تحلیل کرده و در صورت مشاهده هرگونه بسته مشکوک، توسط دیواره آتش از ورود آن به شبکه جلوگیری می‌کند. در واقع عمل واکنش در برابر تشخیص رفتارهای مشکوک، چیزی است که IDS ندارد. کارایی بالای IPS برای

[۱] Wireless-based IDS(WIDS)
[۲] Network Behavior Analysis(NBA)
[۳] Header
[۴] Payload

شبکه‌ها، امری بسیار ضروری است. زیرا ضعف آن‌ها سبب آسیب رساندن به کل شبکه می‌گردد. عمل اصلی در IPSها، تطابق الگو[۱] برای یافتن رشته حملات موجود در پایه‌بار بسته‌هاست. مهم‌ترین عامل در قدرت یک IPS بهره‌مندی از یک موتور تطابق الگوی قوی با سرعت بسیار بالا است. بر طبق نتایج محققان امنیت، این موتور تطابق الگو، باید دارای ویژگی‌های زیر باشد تا به یک مؤلّفه مؤثر IPS تبدیل گردد:

۱. تعداد الگوهای موجود در آن زیاد باشد.

۲. تنوع الگوهای موجود در آن زیاد باشد.

۳. الگوهای رشته‌ای موجود در آن، حساس به متن نباشد.

۴. از سرعت تطابق الگوی بالایی برخوردار باشد.

۵. از الگوهای مبتنی بر پروتکل و مبتنی بر شماره مبدأ و مقصد پشتیبانی گردد.

۶. کارایی بالایی داشته باشد یعنی عملکرد آن متناسب با سرعت شبکه باشد.

۷. پایگاه داده الگوها با سرعت بالا و بدون وقفه بروزرسانی گردد.

تکنیک‌های مختلفی برای ساخت الگو در سامانه‌های IPS معرفی شده است که برخی از مهم‌ترین آن‌ها در [۱۲] آمده است. بنابراین IPS قادر خواهد بود تا جلوی حمله را گرفته و از گسترش و تخریب‌های بعدی ناشی از آن جلوگیری کند. در ادامه تمرکز اصلی ما بر روی سیستم‌های نوظهوری است که عملکرد متفاوتی نسبت به IDSو IPS دارند و عمل پیش‌بینی زودهنگام رخ‌دادهای امنیتی در آن‌ها، مهم‌ترین نقش را ایفا می‌کند. ضمن اینکه این سیستم‌ها به نسبت IDS و IPS گستره بزرگتری از یک شبکه مثلا به اندازه یک کشور یا یک قاره و حتی کل دنیا را تحت پوشش قرار می‌دهند. در ادامه بر روی EWS متمرکز می‌شویم.

سیستم‌های هشدار زودهنگام پس از سیستم‌های تشخیص نفوذ و سیستم‌های جلوگیری از نفوذ، افق جدیدی را برای امنیت اطلاعات و سامانه‌ها و شبکه‌های کامپیوتری ترسیم کرده‌اند[۱۳]. این سامانه‌ها، اطلاعات ورودی خود را با توجه به هدفی که دنبال می‌کنند، از چندین حس‌گر نفوذ تعبیه شده در گره[۲]های شبکه تحت پوشش جمع‌آوری می‌کنند و سپس با تحلیل حجم عظیمی از هشدارهای نفوذ سطح پایین، گزارش‌های نفوذ سطح بالایی را برای مدیران امنیتی فراهم می‌نمایند.

۴.۲ خلاصه فصل

در این فصل، به بررسی مفهوم سامانه هشدار زودهنگام پرداختیم. ابتدا ضمن بیان اهمیت و جایگاه این سامانه‌ها در زمینه امنیت شبکه، آن‌ها را از سیستم‌های مکمل آن‌ها در این زمینه یعنی سیستم‌های تشخیص نفوذ و سیستم‌های پیش‌گیری از نفوذ تمیز دادیم. سپس مهم‌ترین حوزه‌هایی را که این سیستم‌ها مورد استفاده قرار گرفته و می‌گیرند را، ضمن بررسی مهم‌ترین پژوهش‌های صورت گرفته، بیان کردیم. در ادامه ابعاد مختلف سامانه‌های هشدار زودهنگام مورد استفاده در حوزه فناوری اطلاعات را تشریح کردیم. در پایان نیز سامانه‌های هشدار زودهنگام معرفی شده از سال ۲۰۰۰ به بعد را از جنبه‌های مختلف دسته‌بندی کرده‌ایم.

[۱] Pattern Matching
[۲] Node

جدول ۲.۲: مقایسه جنبه‌های مختلف سیستم هشدار زودهنگام با IDS و IPS

	IDS	IPS	EWS
عملکرد	تحلیل ترافیک شبکه و ثبت رخدادهای نفوذ	تشخیص رویدادهای امنیتی، تولید گزارش مناسب و انجام واکنش درخور	تحلیل شواهد نفوذ در یک شبکه وسیع، تولید گزارش، انجام واکنش و پیش‌بینی از آینده و ارسال هشدار زودهنگام به سایر گره‌ها
لایه OSI	۳	۲، ۳، ۴ و ۷	۲، ۳، ۴، ۵، ۶ و ۷
اندازه شبکه	PAN، LAN، WAN	PAN، LAN، WAN	PAN، LAN، MAN، WAN
مؤلّفه‌ها	عامل، حس‌گر، کارگزار مدیریتی، کارگزار پایگاه داده	عامل، حس‌گر، کارگزار مدیریتی، کارگزار پایگاه داده، تحلیل‌گر اثر	عامل، حس‌گر، کارگزار مدیریتی، کارگزار پایگاه داده، تحلیل‌گر اثر، تحلیل‌گر پیش‌بینی
حوزه عملکرد	میزبان، زیرشبکه، کلاینت $WLAN$	میزبان، زیرشبکه، کلاینت $WLAN$	میزبان، عامل شبکه EWS، زیرشبکه EWS
رویه تشخیص	مبتنی بر امضاء، مبتنی بر ناهنجاری، مبتنی بر تحلیل پروتکل حالت‌مند	مبتنی بر امضاء، مبتنی بر ناهنجاری، مبتنی بر تحلیل پروتکل حالت‌مند	مبتنی بر امضاء، مبتنی بر ناهنجاری، مبتنی بر تحلیل پروتکل حالت‌مند
عناصر اطلاعاتی	میزبان‌ها، ترافیک شبکه، رویدادنامه[آ]های سیستم عامل، رویدادنامه‌های برنامه کاربردی، خدمات پروتکل	میزبان‌ها، ترافیک شبکه، رویدادنامه‌های سیستم عامل، رویدادنامه‌های برنامه کاربردی، خدمات پروتکل	میزبان‌ها، ترافیک شبکه، رویدادنامه‌های سیستم عامل، رویدادنامه‌های برنامه کاربردی، رویدادنامه‌های حس‌گرها، خدمات پروتکل
نوع واکنش	تولید هشدار نفوذ	تولید هشدار نفوذ و قدرت بازدارندگی	تولید هشدار نفوذ و قدرت بازدارندگی و پیش‌بینی آینده
نوع معماری	شبکه مدیریت شده و شبکه استاندارد	شبکه مدیریت شده و شبکه استاندارد	توزیعی از شبکه مدیریت شده و یا شبکه استاندارد
یکسانی حس‌گرها	یکسان در حالت توزیعی بودن	یکسان در حالت توزیعی بودن	یکسان، متفاوت
حالت رخداد	غیرفعال	غیرفعال	فعال
قدرت مسدودکنندگی	ندارد	دارد	دارد
پیش‌بینی آینده	ندارد	ندارد	دارد

[آ] Log

جدول ۳.۲: مشخصات فنی و عملکردی سیستم‌های هشدار زودهنگام تجاری

	VDI [۱۴]	ISC [۱۵]	$GEWIS$ [۱۶]	$SADS$ [۱۷]	$VeriSign$ [۱۸]
نظارت					
شبکه	✓	✓	✓	✓	✓
میزبان				✓	
برنامه کاربردی				✓	
جنبه‌های کلی					
سال	۲۰۰۰	۲۰۰۱	۲۰۰۲	۲۰۰۳	۲۰۰۳
کشور	نروژ	آمریکا	آمریکا	آمریکا	آمریکا
حوزه عملیاتی	کشور	چند کشور	کشور	کشور	کشور
حس‌گرها	جریان‌های شبکه	دیواره آتش، ضدویروس، تله‌عسل و IDS	جریان‌های شبکه	دیواره آتش، ضدویروس، تله‌عسل و IDS	جریان‌های شبکه
در دسترس بودن نتایج	خصوصی	خصوصی	خصوصی	عمومی	خصوصی
قابلیت استفاده	✓	✓	✓	✓	✓
شیوه اطلاع‌رسانی	وب‌سایت و گزارش‌ها	وب‌سایت	وب‌سایت و گزارش‌ها	وب‌سایت و گزارش‌ها و پیام کوتاه	وب‌سایت
جمع‌آوری داده					
همکاران	$CERT$ها و $CIIP$	$CERT$ها و سازمان‌های عضو	سازمان‌های عضو	دولت، $CERT$ها و کاربران نهایی عضو	سازمان‌های عضو
جمع‌آوری بلادرنگ رویدادها		✓			✓
معماری	توزیع‌شده	توزیع‌شده	توزیع‌شده	سلسله‌مراتبی	متمرکز
حریم خصوصی	✓	✓			
جنبه‌های فنی					
مبتنی بر ناهنجاری	✓	✓	✓	✓	✓
مبتنی بر امضا		✓		✓	
الگوی حمله		✓		✓	
پاسخ بلادرنگ		✓		✓	
تحلیل پایه‌بار	✓	✓	✓	✓	✓
اهداف	تهدیدات بالقوّه آسیب‌پذیری‌ها کدهای مخرب جدید	کرم‌های جدید شبکه‌های بات آسیب‌پذیری‌ها	$DNSFlooding$ حمله منع سرویس کرم‌های توزیع‌شده	کدهای مخرب جدید حملات $ZeroDay$ استثماری‌های جدید تهدیدات بالقوّه	ویروس‌ها و کرم‌های توزیع‌شده

فصل ۳

همبسته‌سازی هشدار

پس از پردازش هشدارهای هر پنجره توالی رویداد رسیده به مؤلّفه همبسته‌سازی، خروجی این مرحله در پایان تحلیل هشدارهای پنجره، علاوه بر یادگیری سناریوی حملات از طریق درج توالی رویدادهای بحرانی در مدل درخت توالی رویداد، بروزرسانی مقادیر ماتریس همبستگی علّی هشدارهاست. این کار با استفاده از دانش آماری استخراج شده در طول پردازش هشدارهای پنجره توالی رویداد جاری و نیز اطلاعات ذخیره شده در پنجره توالی رویدادهای قبل (به اندازه ضریب پس‌نگری) صورت می‌گیرد. نحوه بروزرسانی CCM در الگوریتم (۳-۱)، نشان داده شده است. یک نکته بسیار مهم درباره عملیات بروزرسانی این است که هم در فرآیند یادگیری حملات در مود برون از خط و هم در فاز تشخیص و پیش‌بینی حملات در مود برخط، این عمل بروزرسانی اعمال خواهد شد تا همواره دانش جدیدی از رفتار مهاجم در دست داشته باشیم.

Algorithm 3.1 CCM Update

Input:

- Rules $a \rightarrow b$ Extracted from Critical Episodes(CE)
- Retrospect Factor (ρ)
- Causal Correlation Matrix (CCM)

Output:

- CCM Update

Algorithm:

LET $1 \leftarrow i\ currentepisodewindownumber$;
LET $a \rightarrow b$ be any tow alert of CE belonging to current episode window;
LET a and b be the first and second alert type of CE;
Generate the rule $a \rightarrow b$;
LET $(timelag(a \rightarrow b)) \leftarrow 0$;
Compute weighted confidence of $(a \rightarrow b)$;
Update $\Psi = a \rightarrow b$;
for $j = 1$ to $min(i-1, \rho)$ **do**
    LET b be any one alert of CE in $episodewindow_i$;
    LET a be any one alert of CE in $\{episodewindow_{i-1}$ or $episodewindow_{i-2}$ or $episodewindow_{i-3}\}$;
    LET a and b b be the alert type of new rule;
    Generate the rule $a \rightarrow b$;
    LET $(timelag(a \rightarrow b)) \leftarrow 0$;
    Compute weighted confidence of $(a \rightarrow b)$;
    Update $\Psi = a \rightarrow b$;
end for

فصل ۴

چارچوب همبسته‌سازی هشدار پیشنهادی

فصل ۵

پیاده‌سازی و ارزیابی

فصل ۶

جمع‌بندی و سوی کارهای آتی

امروزه، طیف گسترده‌ای از تهدیدات اینترنتی برای رسیدن به مقاصد مهاجمان وجود دارد. استفاده از سیستم‌های تشخیص نفوذ برای برقراری امنیت اطلاعات در بستر شبکه‌های کامپیوتری امری انکارناپذیر است. با این حال متخصصان امنیت به راهکارهای پیش‌گیری بسنده نکرده و ورود به عرصه‌ای دیگر از تجهیزات امنیتی که به‌عنوان راهکارهای واکنشی درنظر گرفته می‌شوند را ضروری می‌بینند. سیستم هشدار زودهنگام یک نیاز ضروری برای امنیتِ اطلاعات موجود در شبکه‌های با مقیاس بزرگ امروزی است. هدف اصلی آن‌ها تشخیص زودهنگام رفتارهای بالقوه سیستم، ارزیابی محدوده فعالیت‌های بدخواهانه و در نهایت نیز اعمال واکنش درخور در برابر هرگونه رخداد امنیتی قابل تشخیص است. سیستم‌های هشدار زودهنگام پس از سیستم‌های تشخیص نفوذ و سیستم‌های جلوگیری از نفوذ، افق جدیدی را برای امنیت اطلاعات و سامانه‌ها و شبکه‌های کامپیوتری ترسیم کرده‌اند. یک سیستم هشدار زودهنگام به‌عوان مکمل سیستم‌های تشخیص نفوذ، رفتارهای ناشناخته‌ی سیستم را که به‌طور بالقوه مضر هستند شناسایی می‌کند، که شناسایی رفتارها بر اساس شاخص‌های اولیه انجام می‌شود.

یکی از مهم‌ترین فرآیندها در این سامانه‌ها برای تشخیص به‌موقع رخدادهای بالقوّه مخرب، همبسته‌سازی هشدار است. همبسته‌سازی هشدارها یکی از حوزه‌های فعال تحقیقاتی در زمینه سامانه‌های تسخیص و پیش‌گیری از نفوذها است. هدف از همبسته‌سازی هشدار به‌دست آوردن اطلاعات مفید و سطح بالاتر از حجم انبوه هشدارهای تولید توسط حس‌گرهای تشخیص نفوذ است. در واقع همبسته‌سازی هشدارها با کاهش نرخ مثبت نادرست هشدارها، کاهش حجم هشدارهای تولیدی توسط حس‌گرهای تشخیص نفوذ، تجمیع آن‌ها، ساخت سناریوی حملات و تحلیل راهبرد آن‌ها، علاوه بر ارائه وضعیت امنیتی سیستم، امکان تصمیم‌گیری درست و به‌موقع را برای مدیر امنیتی شبکه فراهم می‌آورد.

در این پایان‌نامه، ضمن بررسی مفاهیم سامانه هشدار زودهنگام و همبسته‌سازی هشدار و ارائه کارهای انجام شده در هر دو زمینه، درکنار تشریح یک سامانه هشدار زودهنگام پیشنهادی با نام $BEWS$، چارچوبی با نام $RTECA$ برای همبسته‌سازی هشدارها ارائه شد. در این چارچوب که هدف اصلی آن استخراج سناریوی حملات چندمرحله‌ای و به‌دست آوردن طرح‌های حمله مهاجم از جریان هشدارهاست، سعی شده است تا با بهره‌گیری از تکنیک‌های آماری و داده‌کاوی، الگوریتمی کارا برای این هدف ارائه شود. از مزایای چارچوب پیشنهادی می‌توان به موارد زیر اشاره کرد:

- **بلادرنگ بودن:** که امکان تصمیم‌گیری به‌موقع را برای مدیر امنیتی شبکه فراهم می‌کند تا با دریافت

اخطارهای زودهنگام، امکان مقابله با حمله و جلوگیری از حملات محتمل بعدی را فراهم آورد.

- **کارایی مناسب:** روش ارائه شده به نسبت روش‌های ارائه‌شده در این زمینه همبسته‌سازش هشدار با هدف تشخیص سناریوی حملات چندمرحله‌ای، زمان بسیار کم و قابل قبولی را برای پردازش جریان هشدارهای دریافتی مصرف می‌کند.
- **تشخیص حملات جدید ناشناخته:** با استفاده از پویاسازی ماتریس همبسته‌سازی هشدار معرفی شده در این پایان‌نامه، قادر به تشخیص سناریوی حملات جدید ناشناخته نیز خواهیم بود.
- **پیش‌بینی گام‌های آتی:** با استفاده از ساخت درخت حمله در مود به‌هنگام و استفاده از دانش یاد گرفته شده از رفتار مهاجم و بروزرسانی آن در مود یادگیری، قادر به ارسال هشدارهای زودهنگام برای پیش‌بینی گام‌های آتی مهاجم است.
- **ترکیب دانش‌ها:** چارچوب ارائه شده برخلاف بسیاری از پژوهش‌های صورت گرفته در این زمینه که برای تعیین علیّت بین هشدارها یا از دانش قبلی موجود در مورد هشدارها و روابط بین آن‌ها استفاده می‌کنند و یا از روابط آماری بین آن هشدارهای تولید بهره می‌برند، از ترکیبی از این دو دانش برای یافتن علیّت بین هشدارها بهره می‌برد تا میزان همبستگی هشدارها را به‌طور کامل‌تر و دقیق‌تری به‌دست آورد.

در این پایان‌نامه از یک مجموعه داده جدید برای ارزیابی کارایی چارچوب همبسته‌سازی $RTECA$ استفاده شده است. در ادمه این پایان‌نامه، جنبه‌هایی از $RTECA$ را که می‌توان بهبود داد عبارتند از:

- **انتخاب دقیق پارامترها و مقادیر اولیه:** با توجه به این‌که در چارچوب $RTECA$ پارامترهای مختلفی به‌کار برده شده است، لذا انتخاب درست آن‌ها اهمیت زیادی پیدا می‌کند که براین این منظور شاید یک راهکار مفید تحلیل حساسیت سیستم به پرامترهای آن است تا به‌صورت دقیق مشخص شود که تغییرات پارامترهای ورودی چه تأثیری بر نتایج همبسته‌سازی خواهد داشت.
- **احتمالاتی کردن مقدار ضریب پس‌نگری:** با توجه به این‌که در این پایان‌نامه ضریب پس‌نگری مقدار ثابتی دارد، بنابراین ممکن است مهاجم با فهمیدن مقدار ضریب پس‌نگری و استفاده از تأخیراندازی بین گام‌های حمله از کشف سناریوی حمله جلوگیری به‌عمل آورد. برای رفع این مشکل می‌توان با استفاده از میزان تغییر هشدارهای در جریان ورودی از یک توزیع احتمالی برای تعیین مفدار مناسب ضریب پس‌نگری بهره برد.
- **امکان حدث حملات از دست رفته:** با افزودن اطلاعات مربوط به آسیب‌پذیری‌ها و نیز حملات چند مرحله‌ای شناخته شده می‌توان قابلیت حدس حملات از دست رفته را به چارچوب معرفی شده افزود.

در بخش اعظمی از این پایان‌نامه نیز به بررسی جنبه‌های سامانه هشدار زودهنگام پرداختیم. مسائل جدید مطرح در زمینه طراحی و توسعه یک سیستم EWS در آینده عبارت‌اند از:

- تولید حس‌گرهای مجازی
- استفاده از راهکارهایی برای حفظ حریم خصوصی داده‌های سازمان‌های عضو
- مدل‌های استدلال جدید برای تحلیل رفتاری شبکه

- استفاده از ترکیب الگوریتم‌های یادگیری کارا برای هوشمند کردن بیشتر سامانه جهت تصمیمات خودکارسازی
- مفاهیم مرتبط با مقیاس‌پذیری، قابلیت اعتماد و انعطاف‌پذیری
- لحاظ کردن شبکه‌های $IPv۶$

[1] Symantec. Internet security threat report. *Technical Report*, 17(2), 2012.

[2] Sophos. Security threat report 2012. *Technical Report*, 2012.

[3] H. J. Liao, C. H. Richard Lin, Y. C. Lin, and K. Y. Tung. Review: Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, 36(1):16–24, 2013.

[4] H. T. Elshoush and I. M. Osman. Alert correlation in collaborative intelligent intrusion detection systems-a survey. *Applied Soft Computing*, 11(7):4349–4365, 2011.

[5] Z. Chenfeng Vincent, L. Christopher, and K. Shanika. Decentralized multi-dimensional alert correlation for collaborative intrusion detection. *Journal of Network and Computer Applications*, 32(5):1106–1123, 2009.

[6] F. Valeur, G. Vigna, C. Kruegel, and R. A. Kemmerer. A comprehensive approach to intrusion detection alert correlation. *IEEE Transaction on Dependable and Secure Computing*, 1(3):146–169, 2004.

[7] R. Sadoddin and A. Ghorbani. Alert correlation survey: Framework and techniques. In *Proceedings of the 2006 International Conference on Privacy, Security and Trust: Bridge the Gap Between PST Technologies and Business Services*, pages 1–10, Ontario, Canada, 2006.

[8] D. G. James. Statistical analysis of internet security threats. *Technical Report*, 2007.

[9] S. R. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles. Botnets: A survey. *Computer Networks*, 57(2):378–403, 2013.

[10] Forest Service. The early warning system for forest health threats in the united states. *Technical Report*, 2000.

[11] Forest Service. The healthy forests initiative and healthy forests restoration act. *Technical Report*, 2003.

[12] D. Stiawan, A. Y. I. Shakhatreh, M. Y. Idris, K. A. Bakar, and A. H. Abdullah. Intrusion prevention system: A survey. *Journal of Theoretical and Applied Information Technology*, 40(1):44–54, 2012.

[13] M. Apel, J. Biskup, U. Flegel, and M. Meier. Towards early warning systems: Challenges, technologies and architecture. In *Proceedings of the 4th International Conference on Critical Information Infrastructures Security*, pages 151–164, Bonn, Germany, 2010.

[14] Norwegian Ministry of Government Administration and Reform. An information society for all. *Technical Report*, 2006.

[15] SANS. About the internet storm center. 2012.

[16] B. Brewin. Feds planning early warning system for internet. 2002.

[17] Symantec unveils global early warning system for internet attacks. 2003.

[18] C. D. Marsan. Verisign aims to give customers early warning of potential attack. 2003.

واژه‌نامهٔ فارسی به انگلیسی

ابرهشدار ..... Meta Alert
آت ..... Oet
ادلکامپ ..... Edelkamp
ارتباط و پاسخ ..... Communication & Responding
ارزیابی و پیش‌بینی تهدید .. Threat Assessment and Prediction
استثمار ..... Exploit
اکتشاف ..... Heuristic
الگو ..... Pattern
الگوهای ترتیبی مکرر ..... Sequential Pattern
آن ..... Ahn
باسیر ..... Bussiere
بدون‌هدف ..... Untargeted
برون‌هسته‌کاوی ..... Outlier Mining
بلادرنگ ..... Real Time
پایگاه داده وقایع و رویدادها ..... Event and Indicator Database
پویش‌های ..... Scan
پیام سیگنالی ..... Signaling Message
پیش‌بینی ..... Prediction
پیش‌گویی ..... Forecasting
پی‌لود ..... Payload
پیمانه‌ای بودن ..... Modularity
تأثیر حمله ..... Attack Impact
تجویز ..... Authorization
تحلیل حالت‌مند پروتکل .... Stateful Protocol Analysis
تحلیل دامنه وسیع ... Domain-Wide Analysis
تحلیل رفتار شبکه ..... Network Behavior Analysis(NBA)
تحلیل شبکه توسعه‌یافته ..... Enterprise-Wide Analysis
تحلیل و اثر ..... Impact & Analysis
تراضی ..... Compromising
تشخیص ..... Detection
تشخیص مبتنی بر امضاء ..... Signature-based Detection
تصدیق هویت ..... Authentication
تطابق الگو ..... Pattern Matching
تغییر منابع سیستم Modification of Resources
تلسکوپ شبکه ..... Network Telescope
توازن بار ..... Load Balancing
توسعه‌پذیری ..... Scalability
تهدیدات ..... Threats
جریان رویدادها ..... Event Stream
جعل ..... Fabrication
جلوگیری از برخورد ..... Conflict Prevention
جمع‌آوری و یادگیری. Collecting and Learning Box
جن ..... Jen
چن ..... Chein
حائل‌شدن ..... Interception
حسابرسی ..... Accounting
حس‌گر ..... Sensor
حس‌گرهای امنیتی ..... Security Appliance Sensors
حس‌گرهای تشخیص الگوی حملات ... Detecting Attack Patterns Sensors
حملات ..... Potential Attacks
حملات منع سرویس توزیع شده ..... Distributed Denial of Service
حملات واقعی ..... Actual Attacks
حوزه حمله ..... Attack Scope
خطرات مربوط به زمین‌شناسی ..... Geological Hazards
دانش اولیه ..... Basic Knowledge
دروازه ..... Gateway
دقت تشخیص ..... Detection Accuracy
دوباره ارسال‌کردن ..... Reply
دی‌بر ..... Debar
دینگ پینگ ..... Dingping

رامانا ..... Ramana
راه‌حل هشدار زودهنگام ..... Early Warning Solution
رخداد ..... Event
رندرز ..... Renders
روش تشخیص سوءاستفاده .. Misuse Detection
روش یکپارچه ..... Monolithic Approach
روش‌های تشخیص رفتار غیرعادی ..... Anomaly-based Detection
زمان‌بر ..... Time Consuming
ژای ..... Zhai
سرآیند ..... Header
سلسله‌مراتبی ..... Hierarchical
سیستم‌های تشخیص نفوذ . Intrusion Detection Systems
سیستم‌های تشخیص نفوذی همکار Co-operative Intrusion Detection Systems
سیستم‌های تصمیم‌یار ..... Decision Support System
سیستم‌های جلوگیری از نفوذ ..... Intrusion Prevention System(IPS)
سیستم‌های هشدار زودهنگام ... Early Warning Systems(EWS)
سیل و طوفان ..... Landslide
سیلوا ..... Silva
شبکه تحقیقاتی آلمان ..... DFN
شبکه‌های بات ..... Botnet
شبکه‌های بزرگ ..... Large Network
شنود ..... Eavesdropping
شیوه حمله ..... Attack Mode
عامل شبکه EWS ..... EWS Network Agent(EWS NA)
غیرفعال ..... Passive
غیرمستقیم ..... Indirect(broad)
فدرال امنیت اطلاعات آلمان Federal Office for Information Security (BSI)
فروچاله نام‌دامنه ..... DNS Sinkhole
فضای تاریک ..... Dark Space
فعالیت‌های بدخواهانه ... Malicious Activities
کارگزار نام‌دامنه Domain Name Service(DNS)
کارگزاران دستور و کنترل ..... C & C Server
کاملا توزیع‌شده ..... Fully Distributed
کانال فرماندهی و کنترل ..... Command and Control (C & C) Channel
کانکوگیل ..... Koyuncugil
کرم های توزیع‌شده ..... Distributed Worms
کرم‌های توزیع‌شده ..... Distributed Worms
کشف و هشدار ..... Detection and Alert
کلایز ..... Claise
کنترل‌کننده بات ..... Botmaster
گسترش بدافزار ..... Malware Spreading
لیائو ..... Liao
لیو ..... Liu
ماشین انرژی هسته‌ای ... Nuclear Power Plant
مبتنی بر ارتباطات بی‌سیم ..... Wireless-based IDS(WIDS)
مبتنی بر اکتشاف ..... Heuristic-based
مبتنی بر الگو ..... Pattern-based
مبتنی بر آمار ..... Statistical-based
مبتنی بر برنامه کاربردی ... Application-based IDS (AIDS)
مبتنی بر حالت ..... State-based
مبتنی بر شبکه .. Network-based IDS(NIDS)
مبتنی بر قانون ..... Rule-based
مبتنی بر میزبان .... Host-based IDS (HIDS)
متخصص ..... Expert
متمرکز ..... Centralized
مثبت غلط ..... False Positive
مثبت-غلط ..... False Positive
مخزن ..... Repository
مرکز حفاظت از زیرساخت‌های اطلاعاتی حساس ... Critical Information Infrastructure Protection(CIIP)
مرکز هشدار زودهنگام ..... Early Warning Center(EWC)
مستقیم ..... Direct
مسدود ..... Block
منفی غلط ..... False Negative
مواد نفتی ..... Oil Spills
موتور همبسته‌ساز ..... Correlator Engine
مولد جریان ..... Stream Generator
ناظر حالت تهدید ..... Threat State Monitor
نظارت و تحلیل .... Monitoring & Analysis
نوع حمله ..... Attack Type
واپاشی ..... Backscatter
واسط ..... Interface
وای ..... Yi
وسیله حمله ..... Attack Means
وقفه ..... Interruption
هدفمند ..... Targeted
هرزنامه ..... Spam

هسته‌ای ..... Nuclear
هش ..... Hash
هشدار زودهنگام ..... Early Warning
هماهنگ‌کننده EWS ..... EWS Coordinator
همبسته‌سازی هشدار ..... Alert Correlation
همکاران ..... Partners
یادگیری ..... Learning

Botnet Early Warning System .... BEWS
Computer Emeregency Response Team . CERT
Healthy Forest Restoration Act ... HFRA
Intrusion Detection Message Exchange Format .... IDMEF
Internet Engineering Task Force ... IETF
IP Flow Information Export ..... IPFIX
ت ..... Patch
Packet Sampling ..... PSAMP
Real Time Episode Correlation Algorithm . RTECA
Support Vector Machine ..... SVM

Abstract

Today, from information security perspective, prevention methods are not enough solely. Early Warning Systems (EWSs) are in the category of reactive methods. These systems are complementing Intrusion Detection Systems (IDSs) where their main goals include early detection of potential malicious behavior in large scale environments such as national level. An important process in EWSs is the analysis and correlation of alerts aggregated from the installed sensors(e.g. IDSs, IP telescopes, and botnet detection systems). In this thesis, beside the definition of a proposed early warning system, an efficient framework for alert correlation in EWSs is proposed. The framework is based on a combination of statistical and stream mining techniques. This process is done in real-time by extracting critical episodes from sequences of alerts, which could be part of multi-step attack scenarios. We also used a Causal Correlation Matrix (CCM) for encoding correlation strength between the alert types in attack scenarios. Experimental results show that the framework is efficient enough in detecting known attack scenarios and new attack strategies. The results also show that the system is able to predict the next steps of the attack up to 95% of accuracy under special circumstances.

Keywords: *Network Security, Early Warning System, Alert Correlation, Multi-step Attack Scenario, Prediction.*

University of Guilan

Faculty of Engineering

Master of Science Thesis
Computer Engineering(Software)

Topic:

Thesis and Scientific Reports Writing Template in LaTeX

By:

Student Name

Supervisors:

Fisrt Supervisor Name
Second Supervisor Name

Mount and Year of Defense