مروری بر همبسته‌سازی هشدارهای امنیتی و بررسی این قابلیت‌ها در سامانهٔ OSSIM

مهدیه صفرزاده واحد[1]، دکتر علیرضا نوروزی[2]، دکتر محمد امین عراقی‌زاده[3]

[1]کارشناسی ارشد، گروه امنیت اطلاعات، دانشگاه صنعتی مالک اشتر، تهران
m.safarzadeh_cn@yahoo.com

[2]استادیار، گروه امنیت اطلاعات، دانشگاه صنعتی مالک اشتر، تهران
nowroozi@mut.ac.ir

[3]دکتری، دانشکده برق و الکترونیک دانشگاه تهران
araghizadeh@ut.ac.ir

چکیده

با افزایش حملات، از سازوکارهای متفاوت در لایه‌های مختلف دفاعی برای تشخیص و جلوگیری از آن‌ها استفاده می‌شود. در این حالت با حجم انبوهی از هشدارها که اطلاعات پراکنده و سطح پایینی دارند، مواجه می‌شویم. یکی از روش‌هایی که برای ترکیب هشدارها و ایجاد دید سطح بالا از وضعیت امنیتی شبکهٔ تحت نظارت، مورد استفاده قرار می‌گیرد، همبسته‌سازی هشدار است. در این زمینه پژوهش‌هایی انجام‌شده است؛ در این مقاله، سامانهٔ OSSIM را معرفی و قابلیت‌های آن را بیان می‌کنیم. با یک رویکرد ترکیبی به مسألهٔ همبسته‌سازی هشدار، دسته‌بندی جدیدی را روی پژوهش‌های علمی انجام داده و با درنظرگرفتن این پژوهش‌ها، فرآیند همبسته‌سازی هشدار در سامانهٔ OSSIM را تشریح و تناظری بین مؤلفه‌های این سامانه و یکی از پژوهش‌ها برقرار کردیم. در اغلب پژوهش‌ها، تمرکز روی همبسته‌سازی هشدارهای سامانه‌های تشخیص نفوذ است؛ ما در این مقاله نشان دادیم که منابع دیگر نیز، در همبسته‌سازی حملات چندگامی مؤثر هستند.

واژگان کلیدی: همبسته‌سازی هشدار، OSSIM، همبسته‌سازی رویداد، حملات چندگامی

۱-مقدمه

با اتصال شبکه‌های رایانه‌ای به یکدیگر و برقراری ارتباط میان آن‌ها و شبکه جهانی اینترنت، بنا به دلایل مختلفی مهاجمان سعی در نفوذ به این شبکه‌ها را داشته و دارند. در طی نفوذ مهاجمان، دارایی‌های اشخاص حقیقی و سازمان‌ها به خطر می‌افتد. برای حفاظت از این دارایی‌ها از دفاع لایه‌ای استفاده می‌شود. در این لایه‌های دفاعی، از ابزارهای مختلف نظارتی و امنیتی، مانند سامانه‌های تشخیص و جلوگیری از نفوذ ماشین میزبان[1] و شبکه[2]، دیوار آتش، ابزارهای ضد بدافزار[3] و ابزارهای رویدادنگار[4] مخصوص تجهیزات شبکه مانند مسیریاب و سوییچ، ابزارهای رویدادنگار سیستم‌عامل مانند Event viewer در ویندوز و Syslog در لینوکس استفاده می‌شود.

هرکدام از این ابزارها با توجه به زمینه‌ای که در آن مورد استفاده قرار می‌گیرند، هشدار[5]ها و رویدادهایی را تولید می‌کنند. تعداد این هشدارها در طول روز به هزاران هشدار نیز می‌رسد. علاوه‌بر تعداد زیاد، این هشدارها شامل هشدارهای مثبت اشتباه[6] و نامرتبط[7] نیز هستند. بنا به دلایل متفاوتی ممکن است، سامانهٔ تشخیص نفوذ، برای حمله هشداری تولید نکند؛ ازجملهٔ این دلایل عدم کارایی، افزایش سرعت تجهیزات شبکه، نبود الگو برای تشخیص حمله را می‌توان نام برد. هشدار و رویدادها بنا به دلایل متفاوتی تولید می‌شوند و هرکدام دید سطح پایینی از وضعیت امنیتی شبکه را گزارش می‌کنند. به‌عنوان‌مثال هنگامی‌که یک حمله چندگامی[8] در حال وقوع است، هرکدام

[1] HIDS
[2] NIDS
[3] Anti Malware
[4] Log

[5] Alert
[6] False Positive
[7] Unrelated
[8] Multi-step Attack

از ابزارهای امنیتی و نظارتی، متناسب با زمینه‌کاری خود، هشدار و یا رویدادهای مرتبط با یک یا چند گام از آن را تولید می‌کنند. برقراری ارتباط بین این هشدار و رویدادهای سطح پایین و استخراج حملات چندگامی از میان آن‌ها توسط مسئول شبکه، امری غیرممکن است. برای رعایت اختصار، در ادامهٔ متن، از هشدار استفاده می‌شود؛ مگر در بخش‌هایی که برای ایجاد تمایز از واژهٔ رویداد استفاده می‌کنیم.

برای برطرف‌کردن و یا کاهش این چالش‌ها، تمام این هشدارها را در یک مرکز عملیات امنیت[1] جمع‌آوری کرده و با اجرای عملیاتی چون همبسته‌سازی هشدار، اولویت‌دهی و مدیریت ریسک روی آن‌ها، گزارش‌های مختلفی چون هشدارهای سطح بالاتر با قابلیت اطمینان و صحت بیش‌تر، برآورد میزان ریسک شبکهٔ تحت نظارت و الگوی حملات چندگامی از آن‌ها استخراج می‌شوند.

در زمینهٔ همبسته‌سازی هشدار در سی سال اخیر، پژوهش‌هایی صورت گرفته است. این پژوهش‌ها منجر به توسعهٔ ابزارهای تجاری و متن‌بازی مانند (OSSIM، Prelude، SIEM، ArcSight، Alert Logic و ...) شده است. علی‌رغم پژوهش‌های صورت‌گرفته، به‌دلیل چالش‌هایی که همچنان حل‌نشده باقی مانده‌اند، مسأله همبسته‌سازی هشدار، همچنان به‌عنوان یک مسألهٔ باز مطرح است. ازجملهٔ این چالش‌ها می‌توان موارد زیر را نام برد:

- حذف و یا کاهش اثر هشدارهای مثبت اشتباه و نامرتبط
- بازیابی هشدارهای منفی اشتباه
- پیش‌بینی گام بعدی حمله
- همبستگی حملات چندگامی به‌صورتی‌که یک یا چندگام از حمله به‌دلیل نبود الگو و یا روز صفربودن حمله قابل‌تشخیص نباشد.
- مسألهٔ پنجرهٔ زمانی
- همبسته‌سازی هشدار و رویدادهای متنوع

در این مقاله یک رویکرد ترکیبی به مسأله همبسته‌سازی هشدار داریم. این راه‌حل را با درنظرگرفتن پژوهش‌های دانشگاهی و ابزارهای فنی توسعه‌داده‌شده در این زمینه مورد بررسی قرار می‌دهیم. یکی از ابزارهایی که در این زمینه توسعه‌داده‌شده است، سامانهٔ OSSIM، برای مدیریت هشدارهای امنیتی است. در ادامه به معرفی این ابزار پرداخته و در مقایسه‌ای بین عملکرد این ابزار و فرآیند همبسته‌سازی هشدار در زمینهٔ دانشگاهی، فرآیند همبسته‌سازی هشدار سامانهٔ OSSIM را تشریح می‌کنیم. تا انتهای مقاله راجع به موارد زیر صحبت می‌شود. در بخش ۲ به معرفی سامانهٔ OSSIM و بیان قابلیت‌های آن می‌پردازیم؛ در بخش ۳ مروری بر فرآیند همبسته‌سازی هشدار و کارهای صورت‌گرفته در زمینه دانشگاهی داریم؛ در بخش ۴ در مقایسه‌ای بین همبسته‌سازی هشدار در سامانهٔ OSSIM و پژوهش‌ها دانشگاهی به تشریح فرآیند همبسته‌سازی در سامانهٔ OSSIM می‌پردازیم؛ در بخش ۵ به بیان نقاط ضعف و قابلیت‌های سامانهٔ OSSIM پرداخته و کارهای آینده را بیان می‌کنیم.

۲-معرفی سامانهٔ OSSIM

OSSIM که مخفف Open Source Security Information Management است، یک راه‌حل امنیتی است که با یک‌پارچه‌کردن مجموعه‌ای از ابزارهای امنیتی و نظارتی و به‌کارگیری الگوریتم‌هایی، به جمع‌آوری و همبسته‌سازی هشدارها و رویدادها پرداخته و گزارش‌های مختلفی از وضعیت امنیتی شبکه تحت نظارت را ارائه می‌کند[۱].

همان‌طور که در شکل شماره ۱ نشان داده‌شده است، این سامانه مجموعه‌ای از هشدارها و رویدادهای متفاوت را از ابزارهای نظارتی و امنیتی دریافت کرده و با اجرای الگوریتم‌هایی روی آن‌ها، گزارش‌های مدیریتی سطح بالاتر و قابل‌فهم‌تر توسط عامل انسانی را ارائه می‌کند.

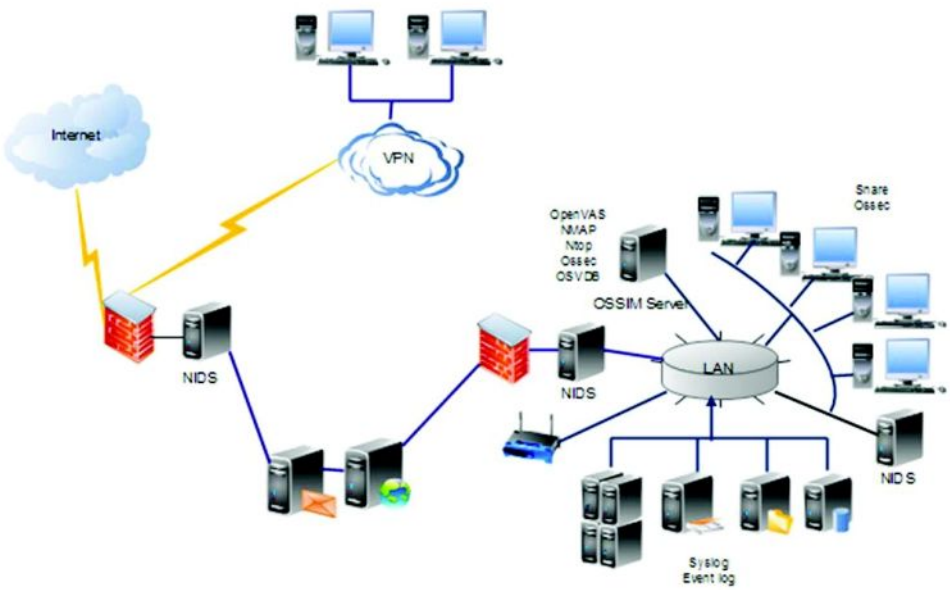
۲-۱-مؤلفه‌های سامانهٔ OSSIM

سامانهٔ OSSIM از ۴ مؤلفه تشکیل‌شده است. در شکل ۲ مؤلفه‌های سامانهٔ OSSIM را ملاحظه می‌کنید.

هرکدام از این مؤلفه‌ها می‌توانند روی یک سامانهٔ مستقل، نصب و سپس با یکدیگر مرتبط شوند؛ یا به‌صورت یک‌پارچه روی یک سامانه قرار گیرند. در ادامه با هرکدام از این مؤلفه‌ها و ابزارهایی که در دستهٔ مربوط به آن‌ها قرار می‌گیرند، آشنا می‌شویم.

۲-۱-۱-Frontend: برای نمایش گزارش‌ها، وضعیت امنیتی شبکه و کاربری راحت‌تر این سامانه، امکان دسترسی تحت وب به آن فراهم شده است. در این محیط نمایش گرافیکی از وضعیت امنیتی شبکه را در قالب‌های مختلف ملاحظه می‌کنید. این امکان را مؤلفه Frontend فراهم می‌کند.

[1] Security Operations Center



شکل ۱: دریافت هشدارها و رویدادهای متفاوت توسط سامانهٔ OSSIM

۲-۱-۲-پایگاه داده: این سامانه از پایگاه داده SQL برای ارزیابی ریسک، همبسته‌سازی و ذخیره‌سازی هشدارها و رویدادهای دریافتی استفاده می‌کند [۲].

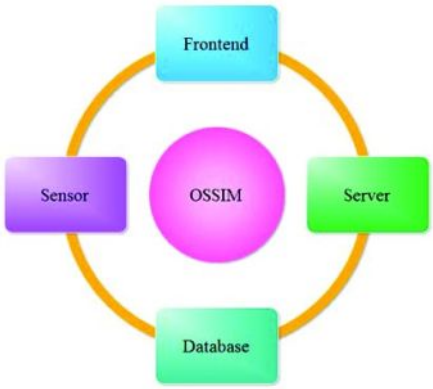
۲-۱-۳-سرور: این مؤلفه خود از دو جزء زیر تشکیل شده است:

- Framework: برای برقراری ارتباط بین چهار مؤلفه بالا مورد استفاده قرار می‌گیرد.
- سرور: اطلاعات را از حس‌گر[1]ها دریافت می‌کند و عملیاتی چون نرمال‌سازی[2]، همبسته‌سازی، اولویت‌دهی به هشدارها، ارزیابی ریسک را انجام می‌دهد. برای محاسبه ریسک سه پارامتر ارزش دارایی[3]، میزان اهمیت تهدید و احتمال رخ‌دادن حمله را در نظر می‌گیرد.

OSSIM به سه صورت همبسته‌سازی هشدار را انجام می‌دهد [۳].

- همبسته‌سازی منطقی[4]
- همبسته‌سازی تقاطعی[5]
- همبسته‌سازی دارایی[6]

[1] Sensor
[2] Normalization
[3] Asset
[4] Logical Correlation
[5] Cross Correlation
[6] Inventory Correlation



شکل ۲: مولفه‌های سامانهٔ **OSSIM**

تشریح کامل فعالیت‌های سرور را در مقایسه‌ای بین نحوهٔ انجام کار OSSIM و پژوهش‌های دانشگاهی در بخش ۴ ارائه می‌کنیم.

۲-۱-۴-حس‌گر: تشخیص‌دهنده[7]گان، ناظر[8]ان و پویشگر[9]ها را که با نظارت بر ترافیک شبکه و پویش در تشخیص‌دهنده[10]گان، ناظر[11]ان و پویش‌گر[12]ها را که با نظارت بر ترافیک شبکه و پویش در محدودهٔ شبکه،

[7] Detector
[8] Monitor
[9] Scanner
[10] Detector
[11] Monitor
[12] Scanner

هشدارهایی را تولید و یا اطلاعاتی را جمع‌آوری می‌کنند، حس‌گر گویند. از حس‌گرها در شبکه برای نظارت‌های گوناگون بر فعالیت‌های شبکه، استفاده می‌شود و نقش جمع‌آوری اطلاعات برای انجام همبسته‌سازی، تولید گزارش و محاسبهٔ ریسک را به عهده دارند. حس‌گرها می‌توانند به‌عنوان سامانهٔ تشخیص نفوذ، پویش‌گر آسیب‌پذیری، تشخیص ناهنجاری[1]، نظارت بر ترافیک شبکه و اتصالات، ابزاری برای ایجاد پروفایلی از سامانه‌های موجود در شبکه و جمع‌آوری هشدار از تجهیزات شبکه مانند مسیریاب و دیوار آتش نقش‌آفرینی کنند. حس‌گرها پس از تولید و یا جمع‌آوری اطلاعات درخواست‌شده آن‌ها را به سرور ارسال می‌کنند.

برخی از این حس‌گرها به‌صورت پیش‌فرض روی خود سامانهٔ **OSSIM** موجود هستند؛ اما می‌توان آن‌ها را روی سامانه‌های مستقل نیز نصب کرد [۴]. در ادامه دسته‌های مختلف حس‌گرها را به‌اختصار معرفی می‌کنیم.

۲-۱-۴-۱-تشخیص‌دهنده‌گان: با دریافت ترافیک و مقایسه با قوانین و الگوهای تعریف‌شده برای آن‌ها، ترافیک حمله را تشخیص و هشداری را در پاسخ به آن تولید می‌کنند. در دستهٔ تشخیص‌دهنده‌گان تشخیص استفادهٔ ننشانیت[2] و تشخیص ناهنجاری هر دو وجود دارند.

۲-۱-۴-۲-ناظران: از ناظران برای بررسی در حال اجرا بودن سرویس‌ها و یا روشن‌بودن ماشین‌های میزبان، کشف ماشین‌های میزبان موجود در محدودهٔ یک شبکه، سرویس‌های در حال اجرا روی یک ماشین میزبان و... استفاده می‌شود. این نظارت در دو سطح زیر صورت می‌گیرد:

- نظارت بر شبکه
- نظارت بر دسترس‌پذیری

۲-۱-۴-۲-۱-نظارت بر شبکه: نظارت بر شبکه برای یک سامانهٔ امنیتی ضروری است. بدون نظارت، مدیر امنیتی قادر نیست فعالیت‌های عادی و غیرعادی را از یکدیگر تمیز دهد و دیدی نسبت به فعالیت‌ها در شبکه ندارد. امکان همبسته‌سازی اطلاعات ناظران و تشخیص‌دهنده‌گان در سامانهٔ OSSIM وجود دارد. نظارت بر شبکه به شیوه‌های زیر صورت می‌گیرد:

- از طریق ایجاد پروفایل‌های روش استفاده و نظارت بر نشست:
  - اطلاعات نحوهٔ استفاده ماشین از شبکه، مانند تعداد بایت‌های ارسال‌شده در طول زمان
  - اطلاعات دربارهٔ فعالیت سرویس‌ها، به‌عنوان‌مثال استفاده از سرویس‌های Mail، pop3 و Http
  - نظارت بی‌درنگ بر نشست، دید کلی از وضعیت نشست‌هایی که میزبان‌ها در آن شرکت می‌کنند ارائه می‌دهد.
- از طریق جریان[3]ها
  - اطلاعات آماری ترافیک مانند مبدأ، مقصد، درگاه‌ها، ترافیک و مدت‌زمان را فراهم می‌کند [۳]

۲-۱-۴-۲-۲-نظارت بر دسترس‌پذیری: اطلاعات دسترس‌پذیری برای تشخیص حملهٔ منع سرویس به‌کار می‌آید. به این منظور، ناظر دسترس‌پذیری Nagios عدم دسترسی به شبکه و ماشین‌های میزبان را بررسی کرده، نمایش و گزارش می‌دهد. سامانهٔ OSSIM با استفاده از پلاگین‌های خود، این اطلاعات را جمع‌آوری کرده و از آن‌ها در فرآیندهای همبسته‌سازی و گزارش‌دهی و تصمیم‌گیری استفاده می‌کند.

۲-۱-۴-۳-پویش‌گران آسیب‌پذیری: پویش‌گران آسیب‌پذیری، امکان بررسی شبکه را ازلحاظ وجود آسیب‌پذیری فراهم می‌کنند. وجود نقاط ضعف را در ماشین‌های میزبان و یا سرورهای شبکه تحت نظارت با انجام حملات شبیه‌سازی‌شده جستجو می‌کنند و آسیب‌پذیری در سطوح شبکه، سرویس و برنامهٔ کاربردی را بررسی می‌کنند. این سامانهٔ امنیتی، ابزارهای نظارتی و امنیتی مختلفی را با یکدیگر یک‌پارچه کرده است که بخشی از آن‌ها در ادامه آورده شده است [۵] .

- سامانهٔ تشخیص نفوذ شبکه: Snort، Cisco ASA و Suricata
- پویش‌گر آسیب‌پذیری: Nessus، OpenVAS

[1] Anomaly Detection
[2] Misuse
[3] Flow

- ناظر شبکه[1]: Ntop
- ناظر دسترس‌پذیری: Nagios
- سامانه‌های تشخیص نفوذ ماشین میزبان: Snare، Osiris و OSSEC
- تشخیص‌دهنده‌های ناهنجاری: Spade و HW Aberant Behaviour
- ناظرانی که به‌صورت غیرفعال کار می‌کنند: Fprobe، Pads، P0f و Arpwatch
- پویش‌گر شبکه: Nmap
- تحلیل‌گر قانونی: Acid/Base
- بعضی از برنامه‌های کوچک دیگر مانند Oinkmaster، PHPAcl، fw1logcheck، ScanMap3D و غیره
- پایگاه داده آسیب‌پذیری: OSVDB

۲-۲- معماری سامانهٔ OSSIM

معماری سامانهٔ OSSIM را در شکل ۳ ملاحظه می‌کنید. همان‌طور که در معماری سامانهٔ OSSIM ، نمایش داده شده است، پردازش‌های زیر در سامانهٔ OSSIM رخ می‌دهد:

- در پایین‌ترین لایه، مجموعه‌ای از تشخیص‌دهنده‌ها قرار دارند که با بررسی ترافیک شبکه و درصورت مشاهده ترافیک مشکوک به حمله یا نقض سیاست‌های امنیتی هشداری را تولید می‌کنند و یا برحسب تقاضا اطلاعاتی را جمع‌آوری می‌کنند.
- سرور، تخمین ریسک، همبسته‌سازی و ذخیرهٔ هشدارها را در یک پایگاه داده SQL انجام می‌دهد.
- سرور، هشدارها را (به همراه امضای دیجیتالشان) درون یک سامانهٔ ذخیره‌سازی بزرگ به‌طور معمول NAS[2] و یا SAN[3] ذخیره می‌کند. (این قابلیت در نسخهٔ تجاری وجود دارد و نام مؤلفه آن logger است.)
- یک واسط کاربر گرافیکی مبتنی بر وب نیز وجود دارد که نتایج عملیات بالا را ارائه می‌کند.

۳- روش‌های همبسته‌سازی هشدار

در این بخش به بررسی و دسته‌بندی پژوهش‌های صورت‌گرفته در زمینهٔ دانشگاهی موضوع می‌پردازیم. همان‌طور که پیش‌تر عنوان شد به‌علت مدیریت و نظارت بر وضعیت امنیتی شبکه‌های رایانه‌ای، پیوسته حجم عظیمی از هشدارها توسط ابزارهای مختلفی که در سطح شبکه به‌کار گرفته می‌شوند، تولید می‌شوند. با توجه به افزایش سرعت در تجهیزات شبکه و سامانه‌های رایانه‌ای و افزایش تهدیدات، تعداد این هشدارها نیز افزایش یافته است. در بخش مقدمه، چالش‌های مطرح در زمینهٔ مدیریت این هشدارها عنوان شد. برای رفع این چالش‌ها راه‌حل همبسته‌سازی هشدار، با قدمتی حدود سی سال، به‌کار گرفته شده است.

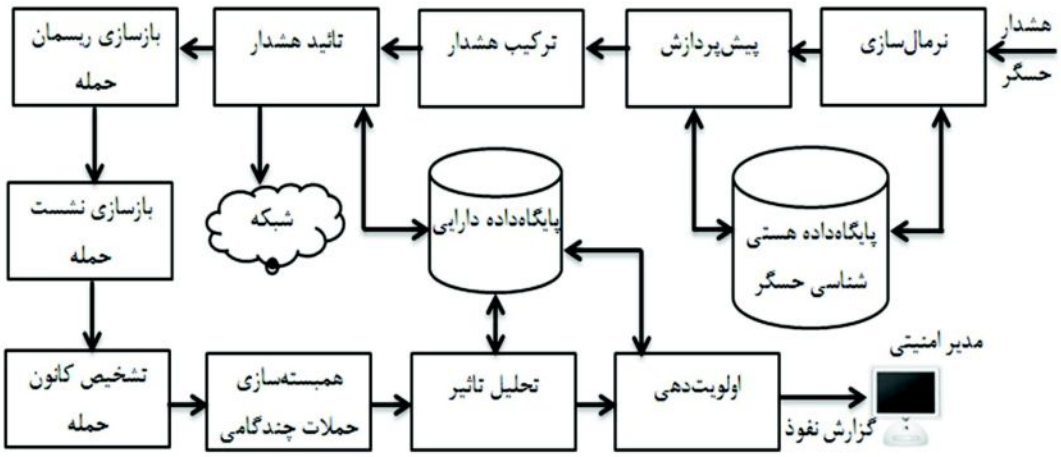
در فرآیند همبسته‌سازی هشدار، اطلاعات و رویدادهای امنیتی از شبکهٔ تحت نظارت جمع‌آوری شده و روی آن‌ها مدیریت و عملیاتی برای کاهش، تأیید، تصحیح، ایجاد ارتباط بین هشدارهای سطح پایین و ایجاد دید سطح بالا صورت می‌گیرد و درنهایت گزارشی از وضعیت شبکهٔ تحت نظارت تهیه و ارائه می‌شود.

شکل ۳: معماری سامانهٔ OSSIM

۳-۱-مؤلفه‌های موجود در مدل والوئر: در یکی از پژوهش‌هایی که در این زمینه صورت گرفته [۶]، والوئر یک رویکرد جامع از همبسته‌سازی هشدار ارائه کرده است. والوئر در این رویکرد، کامل‌ترین دید را نسبت به فرآیند همبسته‌سازی هشدار داشته است.

در این رویکرد همان‌طور که در شکل ۴ ملاحظه می‌کنید، طی ده مرحله عملیاتی روی هشدارهای خام صورت می‌گیرد و درنهایت هشدار سطح بالایی به مسئول امنیتی شبکه، گزارش می‌شود.

[1] Network Monitor
[2] Network Attached Storage
[3] Storage Area Network



شکل ۲-۳: مؤلفه‌های فرآیند همبسته‌سازی هشدار [۱]

۳-۱-۱-مؤلفهٔ نرمال‌سازی: قالب هشدارهای خام دریافتی از تجهیزات امنیتی و نظارتی گوناگون، با یکدیگر متفاوت است. برای ایجاد قابلیت مقایسهٔ میان آن‌ها، تمام هشدارها توسط مؤلفهٔ نرمال‌سازی به قالب استاندارد IDMEF [۷] تبدیل شده و به مؤلفهٔ پیش‌پردازش ارسال می‌شوند.

۳-۱-۲-مؤلفهٔ پیش‌پردازش[1]**:** ممکن است هنگام تولید هشدار در برخی از فیلدها مقداری درج نشود، در این مؤلفه درصورتی‌که فیلدهای موجود در قالب استاندارد IDMEF بدون مقدار باشند، با رعایت شرایطی به‌روزرسانی می‌شوند. سپس هشدار به مؤلفه ترکیب هشدار وارد می‌شود.

۳-۱-۳-ترکیب هشدار[2]**:** همان‌طور که پیش‌تر مطرح شد، در سطح شبکه، از ابزارهای مختلفی که هرکدام در یک دسته خاصی قرار دارند، استفاده می‌شود. ممکن است در یک دسته از دو یا چند ابزار مختلف استفاده شود به‌عنوان‌مثال اگر بیش از یک برنامه ضد بدافزار در سطح شبکه به کار گرفته شود، این دو ضد بدافزار برای اغلب بدافزارها هشدارهای یکسان تولید می‌کنند. ما برای تشخیص این بدافزارها تنها به یک نمونه از این هشدارها نیاز داریم. این مؤلفه، هشدارهای مشابه تولیدشده توسط دو یا چند ابزار متفاوت که در یک دسته مشابه قرار دارند را، با یکدیگر ترکیب می‌کند.

۳-۱-۴-تأیید هشدار[3]**:** در مؤلفهٔ تأیید هشدار، با استفاده از روش‌هایی، درستی هشدار بررسی می‌شود؛ در این مرحله هشدارهای مثبت ننشانیت و مثبت نامرتبط حذف می‌شوند. این مؤلفه تأثیر هشدارهایی که تشخیص حملات را به مسیر اشتباهی هدایت می‌کنند، کاهش می‌دهد.

۳-۱-۵-بازسازی ریسمان حمله[4]**:** یک مهاجم ممکن است سوء استفادهٔ خاصی را علیه یک ماشین مشخص با پارامترهای مختلفی مورد بهره‌برداری قرار دهد. در این حالت به‌ازای هر بار تغییر پارامتر، یک هشدار تولید می‌شود. این هشدارها به‌دلیل حملهٔ یک مهاجم مشخص به یک ماشین میزبان مشخص تولید می‌شوند. در مؤلفهٔ بازسازی ریسمان حمله، این هشدارها با یکدیگر ترکیب و همبسته می‌شوند.

۳-۱-۶-بازسازی نشست حمله[5]**:** برخی از هشدارهای تولیدشده توسط سازوکارهای تشخیص در سطح شبکه تولید می‌شوند و برخی در اثر سازوکارهای تشخیص روی ماشین میزبان، مؤلفهٔ بازسازی نشست حمله این دو دستهٔ هشدار را با یکدیگر ترکیب می‌کند.

۳-۱-۷-تشخیص کانون حمله[6]**:** در شبکه‌های رایانه‌ای ممکن است حملات توزیع‌شده رخ دهد. این حملات به دو

[1] Pre-Processing
[2] Alert Fusion
[3] Alert Verification
[4] Thread Reconstruction
[5] Attack Session Reconstruction
[6] Focus Recognition

دسته تقسیم می‌شوند: حملات چند به یک[1]، در این حملات چند ماشین میزبان به یک ماشین میزبان حمله می‌کنند و دسته دوم حملات یک به چند[2]، یک ماشین میزبان چند ماشین میزبان را مورد حمله قرار می‌دهد. این نوع حملات توزیع‌شده توسط مؤلفهٔ تشخیص کانون حمله، با همبسته‌سازی هشدارهای مربوط به آن‌ها شناسایی می‌شوند.

۳-۱-۸-همبسته‌سازی حملات چندگامی[3]: حملاتی که صورت می‌گیرند از بیش از یک گام تشکیل شده‌اند. گام‌های تشکیل‌دهنده اغلب به‌صورت شکل شمارهٔ ۵ دسته‌بندی می‌شوند[۸]. در مؤلفه همبسته‌سازی حملات چندگامی گام‌های هر حمله با یکدیگر همبسته می‌شوند.

شکل ۵: گام‌های تشکیل‌دهنده یک حمله چندگامی

۳-۱-۹-تحلیل اثر[4]: در ادامه و پس از شناسایی الگوی سطح بالای حمله، مؤلفهٔ تحلیل اثر، تأثیر هر رویداد را بر شبکه تحت نظارت بررسی می‌کند.

[1] Many2One
[2] One2Many
[3] Multi-step Correlation
[4] Impact Analysis

۳-۱-۱۰-اولویت‌دهی[5]: در مؤلفهٔ نهایی، بر اساس سیاست‌های سازمان به هشدارها اولویت تخصیص می‌یابد. در زمینهٔ هرکدام از مؤلفه‌های نامبرده، پژوهش‌هایی صورت گرفته است. در ادامهٔ این بخش، پژوهش‌های انجام‌شده را با رویکرد نمایش‌داده‌شده در شکل ۶ بررسی می‌کنیم.

۳-۲- انواع مدل

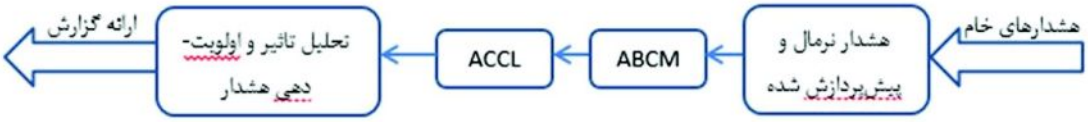
والوئر و همکاران در [۶] رویکردی را ارائه کردند که شرح آن را در بخش۳ آوردیم. A.E. Taha و همکارانش در [۹] با انجام تغییراتی در رویکرد والوئر رویکرد خود را ارائه کردند. در این رویکرد پس از دریافت هشدار، با استفاده از یک عامل یادگیرنده به نام ABCM، حداقل تعداد مؤلفه‌های مؤثر و مفید برای پردازش این هشدار و ترتیب اجرای این مؤلفه‌ها به مؤلفهٔ ACCL ارسال می‌شود. انتخاب مؤلفه با توجه به هشدارهای دریافتی پیش از این هشدار صورت می‌گیرد. این امر باعث می‌شود در هر مؤلفه کم‌ترین تعداد هشدار پردازش شده و درنتیجه زمان همبسته‌سازی هشدار کاهش یافته و کارایی در مجموع افزایش می‌یابد. مراحل انجام کار در شکل ۷ نمایش داده شده است.

Elshoush و همکارش در [۱۰] نیز ترتیب مؤلفه‌های والوئر را به‌شکلی که مؤثرتر واقع شوند تغییر داده و مؤلفه‌های حذف هشدارهای همبسته‌نشده و تشخیص قصد مهاجم را به آن اضافه کرده‌اند.

- مؤلفهٔ حذف هشدارهای همبسته‌نشده، هشدارهای مثبت اشتباه و نامرتبط را حذف می‌کند.
- مؤلفهٔ تشخیص قصد مهاجم، اهداف و استراتژی‌های یک مهاجم را بر اساس سناریوی حملات با در نظر گرفتن عملیاتی که مهاجم انجام داده استنباط می‌کند. مدل پیشنهادی آن‌ها در شکل ۸ نمایش داده شده است.
- برای اشتراک اطلاعات، پهنای باند بیشتری را مصرف می‌کند.
- دید کلی از شبکهٔ تحت نظارت ارائه نمی‌کند.
- توازن بار در آن باید صورت گیرد، به‌طوری‌که همهٔ عامل‌ها به نسبت یکسانی هشدارها را همبسته کنند[۱۴].

[5] Prioritization

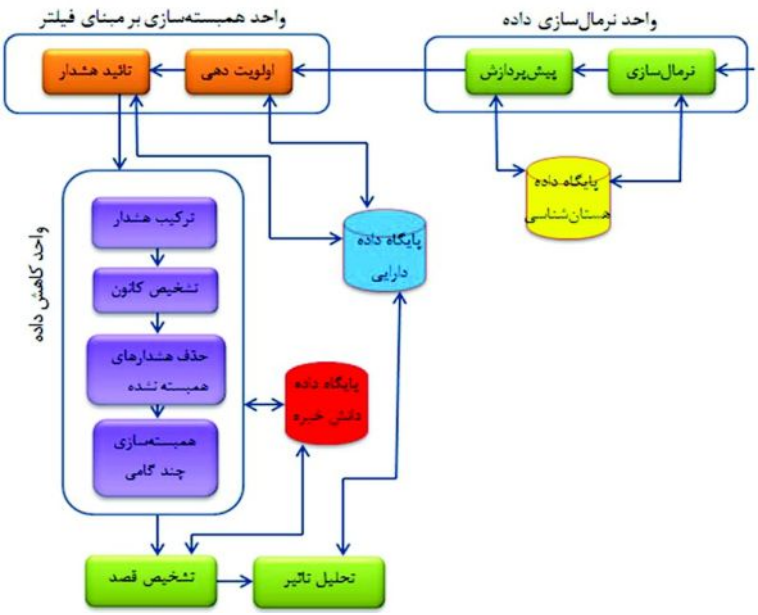
شکل ۶: دسته‌بندی پژوهش‌های صورت گرفته در زمینه همبسته‌سازی هشدار



ABCM: Agent Based Correlation Model ACCL: Active Correlation Components List

شکل ۷: مؤلفه‌های پیشنهادی در [۹]

۳-۳-۳-سلسله‌مراتبی: معماری سلسله‌مراتبی در طراحی خود از معماری توزیع‌شده بهره برده است. در این معماری، عامل‌های مدیریتی به سطوح مختلفی تقسیم می‌شوند و با عامل‌های نظیر خود به‌صورت افقی و با عامل‌های دیگر به‌صورت عمودی در ارتباط‌اند. نتایج همبسته‌سازی خود را به عامل‌های سطح بالاتر ارسال می‌کنند. هر عامل هشدارهای دریافتی خود را در کنار نتایج دریافتی توسط عامل‌های زیرمجموعهٔ خود همبسته می‌کند. تا زمانی که درنهایت اطلاعات به عامل ریشه ارسال شود؛ عامل ریشه، یک دید کلی از وضعیت شبکه تحت نظارت با استفاده از دیدهای سطح پایین، ایجاد می‌کند [۱۴]. می‌توانیم معماری سلسله‌مراتبی را ترکیبی از دو معماری قبلی بدانیم. T. Donghai و همکاران [۱۵] الگوریتم همبسته‌سازی سلسله‌مراتبی را ارائه کرده‌اند که شامل سه مرحله است: در مرحلهٔ نخست هشدارها با یکدیگر ترکیب می‌شوند؛ سپس برخی از عامل‌های همبسته‌سازی به‌صورت محلی گراف همبسته‌سازی هشدار خود را ایجاد کرده و در مرحله آخر واحد همبسته‌سازی مرکزی گراف کلی همبسته‌سازی هشدار را با استفاده از نتایج محلی دریافت‌شده ایجاد می‌کند.



شکل ۸: مؤلفه‌های پیشنهادی در [۱۰]

۳-۴-زمینه‌های کاربرد

همبسته‌سازی هشدارها در سه زمینهٔ مدیریت شبکه، امنیت فناوری اطلاعات و سامانه‌های کنترل صنعتی[1] مورد استفاده قرارگرفته است که در ادامه به‌اختصار بیان می‌شوند.

۳-۴-۱-مدیریت شبکه

سامانهٔ مدیریت شبکه[2] (NMS) توسط اپراتورها استفاده می‌شود تا کارهای مدیریتی را انجام دهند. کارهایی چون مدیریت پیکربندی شامل تنظیمات دستگاه‌ها، مدیریت خطا که از عهده خطاها برمی‌آید و تأثیرات و راه‌حل‌های آن‌ها را بررسی می‌کند؛ مدیریت کارایی که وضعیت شبکه و برخی مسائل کارایی را نظارت می‌کند و مدیریت‌های دیگر چون حسابرسی و امنیت.

عامل‌ها و فرآیندها روی تجهیزاتی[3] که قرار است مدیریت شوند، اجرا می‌شوند و اطلاعات را جمع‌آوری و تحت عنوان هشدار به مدیر می‌فرستند. سپس روی آن‌ها پردازش‌هایی صورت گرفته و به اپراتور نمایش داده می‌شود. در زمینه مدیریت شبکه، همبسته‌سازی هشدار استفاده می‌شود، تا به اپراتور در تشخیص کمک کند و به فرآیند مکان‌یابی خطا سرعت ببخشد. در این زمینه در [۱۶] پژوهشی انجام شده است.

۳-۴-۲-امنیت فناوری اطلاعات

بیشترین پژوهش‌ها در همین زمینه انجام‌شده است. این پژوهش‌ها روی همبسته‌سازی هشدارهای سیستم‌های تشخیص نفوذ صورت گرفته است. پژوهش‌ها کمی نیز بر روی همبسته‌سازی هشدارهای سیستم‌های تشخیص نفوذ و سایر هشدارهای مطرح‌شده در بخش ۳-۴ تمرکز کرده‌اند. از همبسته‌سازی هشدار برای تأیید اعتبار هشدارها و تشخیص سناریوهای حملات چندگامی و پیچیده استفاده می‌شود.

۳-۴-۳-سیستم‌های کنترل صنعتی

علاوه بر دو زمینه فوق در بخش‌های صنعتی نیز همبسته‌سازی هشدار برای بهبود کنترل فرآیند خودکارسازی بکار گرفته می‌شود. در اکثر سیستم‌های کارخانه‌ای تعداد زیادی سوئیچ و حس‌گر فعال‌کننده وجود دارد که می‌توانند حجم عظیمی از هشدارها را در پاسخ به اخلال یا خطا تولید کنند. سیستم‌های مدیریت هشداری وجود دارند که به کمک روش‌های همبسته‌سازی هشدار به کشف علل ریشه‌ای مشکلات کمک می‌کنند. تحقیق [۱۷] در همین راستا انجام‌شده است.

[1] SCADA
[2] Network Management System
[3] Device

۳-۵- انواع منابع

هشدارهای تولیدشده توسط سامانه‌های تشخیص نفوذ، اصلی‌ترین منبع اطلاعاتی است که باید به تمام سامانه‌های همبسته‌سازی هشدار، ارائه شود. اما منابع دیگری نیز وجود دارند که می‌توانند برای افزایش دقت و کارایی و تشخیص در فرآیند همبسته‌سازی، مشارکت کنند. برخی حملات تنها توسط یک منبع قابل‌شناسایی نیستند، و برای تشخیص به اطلاعات بیش از یک منبع نیاز است [۱۸و۱۹و۲۰]، به همین علت برای تشخیص آنها لازم است تا از منابع متفاوت در کنار یکدیگر بهره ببریم. از این منابع در اکثر مؤلفه‌ها استفاده می‌شود. در اینجا انواع منابع را طبقه‌بندی و معرفی می‌کنیم [۲۱] و [۲۲]. انواع مختلف این هشدارها را می‌توان در دسته‌های زیر جای داد:

جدول ۱: دسته‌بندی انواع منابع مناسب برای همبسته‌سازی هشدار

سامانهٔ تشخیص نفوذ	سامانهٔ تشخیص نفوذ ماشین میزبان
	سامانهٔ تشخیص نفوذ شبکه
سیستم‌عامل	رویدادهای امنیتی[1]
	رویدادهای سیستمی[2]
	رویدادهای برنامه‌های کاربردی
رویداد برنامه‌های کاربردی	سرور وب
	سرور پایگاه داده
	سرور ایمیل
	سرور نام دامنه
	سرور اشتراک فایل
تجهیزات شبکه	سوئیچ
	مسیریاب
	دیوار آتش
	نقاط دسترسی بی‌سیم[3]
ابزارهای فیزیکی	دوربین
	سامانه‌های کنترل دسترسی[4]

[1] Security Log
[2] System Log
[3] Wireless Access Point
[4] Access Control System

سه دسته رویداد مرتبط با سیستم‌عامل در نتیجهٔ عملیات زیر تولید می‌شوند[۲۱]:

- احراز اصالت: ورود و خروج
- اجرای دستورهای دارای مجوز
- روشن و خاموش‌شدن و راه‌اندازی دوباره سیستم
- راه‌اندازی و خاموش‌شدن و تغییر وضعیت سرویس
- فعالیت‌های سرویس‌ها و پیغام‌های خطا

منابع دیگری نیز در همبسته‌سازی هشدار مورداستفاده قرار می‌گیرند که عبارت‌اند از:

- فایل‌های مشخصات پیکربندی سیستم‌ها و به‌هم‌بندی شبکه
- اطلاعات آسیب‌پذیری سیستم‌ها و یا تجهیزات شبکه
- سیاست‌های امنیتی سازمان

۳-۶-روش‌های همبسته‌سازی هشدار

روی روش‌های همبسته‌سازی هشدار دسته‌بندی‌های مختلفی انجام‌شده است. یکی از این دسته‌بندی‌ها که تقریباً تمام روش‌ها را پوشش می‌دهد عبارت است از:

- روش مبتنی بر شباهت[5]
- روش پیش‌نیاز/نتیجه[6]
- روش مبتنی بر سناریوهای حمله ازپیش تعریف‌شده[7]

پژوهش‌های فراوانی در زمینهٔ همبسته‌سازی هشدار انجام‌شده است؛ به‌دلیل اینکه برای تشخیص حملات تنها تمرکز بر یکی از دسته‌های تشخیص یعنی سامانهٔ تشخیص نفوذ کافی نیست، در این مقاله بیشتر، روی پژوهش‌های تمرکز می‌کنیم که هشدارهای تولیدشده توسط دسته‌های متفاوت تشخیص حملات و رفتار مخرب را همبسته کرده‌اند.

۳-۶-۱-روش مبتنی بر شباهت

روش مبتنی بر شباهت، هشدارها را با استفاده از شباهت‌هایی که با یکدیگر دارند دسته‌بندی می‌کند. هر هشدار که تولید می‌شود چندین صفت یا فیلد دارد، مانند نشانی‌های IP مبدأ و مقصد، شمارهٔ درگاه‌های مبدأ و

[5] Similarity Based
[6] *Prerequisite-Consequence*
[7] Predefined Attack Scenarios

مقصد، نوع پروتکل، شرح هشدار و مهر زمانی[1]. فرض اصلی در اینجا این است که هشدارهای مشابه علل ریشه‌ای مشابه و یا تأثیر مشابهی بر سامانهٔ تحت نظارت دارند. روش‌های مبتنی بر شباهت خود به دو دستهٔ زیر تقسیم می‌شوند:

۳-۶-۱-۱-روش مبتنی بر شباهت صفات

روش همبسته‌سازی مبتنی بر صفات، هشدارها را با استفاده از شباهت بین صفات یا ویژگی‌های آن‌ها همبسته می‌کند. به این منظور چندین ویژگی مانند: نشانی‌های IP مبدأ و مقصد، مهرهای زمانی، شماره‌های درگاه ، نوع سرویس و کاربر می‌تواند مورد استفاده قرار گیرد. معیار شباهت به‌وسیلهٔ معیارهای خاص محاسبه، مانند توابع فاصلهٔ منهتن۲، اقلیدسی۳، ماهالانوبیس۴، و مینوفسکی۵ محاسبه می‌شود. نتایج به‌دست‌آمده در مقایسه با مقادیر آستانه‌ای تعریف‌شده، تعیین می‌کنند که آیا هشدارها با یکدیگر همبسته شوند یا خیر. انتخاب معیار فاصلهٔ مناسب، کارایی کلی فرآیند همبسته‌سازی را افزایش می‌دهد. اینکه دو هشدار به یکدیگر شباهت دارند یا خیر، براساس تابع فاصله در نظر گرفته می‌شود[۱۴]. این روش در زمینهٔ تئوری، در پژوهش‌ها زیادی مورد استفاده قرارگرفته است، بیش‌ترین پیاده‌سازی هم در همین بخش صورت گرفته است. همه این روش‌ها از یک معیار شباهت برای همبسته‌سازی استفاده می‌کنند؛ اما تفاوت‌های زیادی در تکنیک‌هایی که برای سنجش میزان شباهت استفاده کرده‌اند، وجود دارد. Valdes و Skinner در [۲۳] یک روش احتمالی برای همبسته‌سازی هشدارها براساس چهارچوب ریاضی تعریف کرده‌اند، که قادر است حداقل شباهت مشخصات را برای ترکیب هشدارهای دریافتی از چندین حس‌گر را به‌دست آورد. از این روش در پژوهش‌ها [۲۴-۲۸] استفاده شده است.

۳-۶-۱-۲-روش مبتنی بر شباهت زمانی

در روش مبتنی بر شباهت، از محدودیت‌های زمانی برای پیداکردن روابط بین هشدارها برای هبسته‌سازی و تجمیع آن‌ها استفاده می‌کنند. روابط زمانی بین هشدارها، اطلاعات ارزشمندی ارائه می‌کنند، که می‌تواند در فرآیند همبسته‌سازی مورداستفاده قرار گیرد. ایدهٔ پشت این روش همبسته‌سازی عبارت است از اینکه هشدارهایی که به‌دلیل یکسانی ایجاد می‌شوند با احتمال زیاد در مدت‌زمان کوتاهی بعد از وقوع خطا مشاهده می‌شوند. ساده‌ترین روش همبسته‌سازی زمانی، بر پنجره‌های زمانی تکیه می‌کند. در این روش تنها هشدارهایی که در یک پنجرهٔ زمانی تولید می‌شوند با یکدیگر همبسته می‌شوند[۱۴].

استحکام ارتباط زمانی بین دو هشدار به دو صورت قوی و ضعیف برچسب‌دهی می‌شود. اگر فواصل زمانی، تاحدودی مقادیر ثابتی داشته باشند، به‌صورت قوی[6] و درصورتی‌که مقدار دقیقی نداشته باشند، آن‌ها را به‌صورت سست[7] برچسب‌دهی می‌کند. از این روش در [۳۲-۲۹] استفاده شده است. مزایا و معایب این روش عبارت‌اند از:

مزایا:

- الگوریتم‌های سبک‌وزن و پیچیدگی کمتر پیاده‌سازی
- کاهش حجم هشدارها

معایب:

- ناتوانی در همبسته‌سازی روابط سببی بین هشدارها

۳-۶-۲-روش پیش‌نیاز-نتیجه

در روش پیش‌نیاز/نتیجه، فرآیند همبسته‌سازی هشدار سعی دارد روابط سببی بین هشدارها را از طریق پیش‌نیاز و نتایج هشدارها پیدا کند. فرض بر این است که هشدارهای قبلی شرایط را برای هشدارهای بعدی فراهم می‌کنند. اگر نتیجهٔ یک هشدار با پیش‌نیاز هشدار دیگر یکی بود، دو هشدار با یکدیگر همبسته می‌شوند.

Xu و Ning در [۳۳] در سه مرحله همبسته‌سازی هشدار را انجام می‌دهند، سازوکارهای امنیتی متفاوت برای یک حملهٔ یکسان، ممکن است هشدارهای متفاوتی تولید کنند؛ اما رویدادهایی که این هشدارها را تولید می‌کنند، باید یکسان باشند؛ بر همین اساس هشدارهایی که رویدادهای تولیدکنندهٔ آن‌ها یکسان هستند در یک دسته قراردادند. به‌این‌ترتیب در مرحلهٔ تخست، هشدارها را دسته‌بندی کردند و هر دسته بیان‌گر یک گام از حمله است. در گام بعد هر دسته را با پیکربندی ماشینی که مورد

[1] Timestamp
[2] Manhattan
[3] Euclidean
[4] Mahalanobis
[5] Minkowski

[6] Strong
[7] Loose

حمله قرارگرفته مقایسه و هشدار را تأیید می‌کنند؛ سپس در گام آخر براساس مدل پیش‌نیاز، نتیجهٔ دسته‌ها را با یکدیگر همبسته می‌کنند.

[۳۴] RIAC[1] یک مدل همبسته‌سازی هشدار بی‌درنگ است و برای تحلیل و کشف سناریوهای حمله، ارائه شده است. فرض اصلی در این روش این است که مؤلفه‌های حمله، مستقل از یکدیگر نیستند؛ بلکه در گام‌های متفاوتی از حمله به یکدیگر وابسته هستند. به این صورت که گام قبلی شرایط را برای گام بعدی فراهم می‌کند. با استفاده از منطق محمولات آن‌ها مفهوم ابر هشدار را برای نمایش پیش‌نیاز و نتیجه هر هشدار ارائه کردند. هر ابر هشدار یک چندتایی به‌صورت (واقعیت[2]، پیش‌نیاز، نتیجه) است. واقعیت، مجموعه‌ای از نام صفات در هشدارهاست. پیش‌نیاز و نتیجهٔ دو مجموعه متفاوت، و هرکدام شامل ترکیب منطقی از مسندات هستند که به‌صورت شرایط ریاضی روی متغیرهایی که در مجموعه واقعیت‌ها وجود دارد، تعریف‌شده‌اند. در [۳۵] کار مشابهی پیاده‌سازی شده است.

Zhou و همکاران در [۳۶] به‌منظور همبسته‌سازی خودکار، هشدارهایی که در جریان یک نفوذ مشخص تولید شده‌اند، مدل خوش‌ساختاری ارائه کردند. در این مدل تمام دسترسی‌هایی که مهاجم در هر گام از یک حمله چندگامی به‌دست می‌آورد، در قالب یک بلوک سازندهٔ پایه به نام قابلیت[3] بیان می‌شود. آن‌ها برای بیان ارتباط منطقی بین قابلیت‌های متفاوت، تعدادی قوانین استنتاجی تعریف کرده و براساس مدل و قوانین استنتاج، الگوریتم‌هایی برای اعمال قوانین روی قابلیت‌ها نوشته و پیاده‌سازی کردند.

در [۳۷] Saad و Traore با استفاده از تحلیل معنا و یک آنتولوژی نفوذ جدید، روشی برای بازسازی سناریوی حملات براساس روابط صریح و ضمنی بین هشدارها ارائه کردند. این روش قادر به بازسازی سناریوی حملات شناخته‌نشده و جدید و همبسته‌سازی هشدارهای تولیدشده در محیطی با چند حس‌گر IDS هست. این روش در [۴۰-۳۸] به‌کار گرفته شده است.

۳-۶-۳-روش‌های مبتنی بر سناریوهای حملهٔ ازپیش‌تعریف‌شده

این روش هشدارها را براساس سناریوی حملات شناخته‌شده همبسته می‌کند. سناریوی حملات یا با استفاده از زبان‌های خاصی مانند STATL، LAMDBA و توسط فرد خبره و یا با استفاده از مجموعه‌داده‌ها و روش‌های داده‌کاوی استخراج می‌شوند. در این دسته، از یک سامانهٔ مبتنی بر پایگاه دانش برای نمایش سناریوها استفاده می‌شود. Eckmann و همکاران در [۴۱] STATL زبان حمله‌ای را براساس انتقال بین وضعیت‌های ماشین میزبان را ارائه کردند. با استفاده از این زبان، ترتیب عملیاتی که یک مهاجم برای نفوذ به یک سامانه انجام می‌دهد، بیان می‌شود.

Dain و همکاران در [۴۲] ویژگی‌های خاصی را انتخاب کرده و سپس روش‌های داده‌کاوی MLP،RBF و درخت تصمیم را روی آن‌ها به‌کار گرفتند.

معایب این روش عبارتند از:

- محدود به حملات شناخته‌شده
- اگر به روش داده‌کاوی همبسته‌سازی انجام شود نمی‌تواند روابط سببی را شناسایی کند.

در [۴۳] Porras و همکارانش روی همبسته‌سازی هشدارهای امنیتی متنوع کارکردند. در این پژوهش هشدارهای امنیتی متنوع براساس صفات مشترک، مانند نشانی IP و شمارهٔ درگاه و نوع حمله در محدودهٔ زمانی نزدیک به یکدیگر دسته‌بندی می‌شوند. هر کدام از این دسته‌ها بیان‌گر یک گام از حمله هستند. این روش تنها برای ترکیب هشدارهای متنوع با یکدیگر استفاده شده است.

۳-۷-فعالیت‌های پس از همبسته‌سازی

۳-۷-۱-تشخیص قصد و منظور: قصد و منظور مهاجم، با مشاهدهٔ عملیاتی که توسط او انجام می‌شود، تشخیص داده می‌شود. مهاجم برای مخفی‌کردن هدف خود رفتار خود را تغییر داده یا به‌صورت مخفیانه عمل می‌کند. همان‌طور که در بخش ۳-۱-۸- بیان شد، مهاجم برای رسیدن به هدف خود چند گام حمله را انجام می‌دهد، با استفاده از همبسته‌سازی هشدار، هشدارهای مربوط به یک سناریوی حملهٔ همبسته‌شده و سپس هدف مهاجم از سناریوهای حملات استخراج می‌شود. Ning و همکاران در [۴۴] روشی را ارائه کردند که با استفاده از یک گراف

[1] Realtime Alert Correlation
[2] Fact
[3] Capability

جهت‌دار بدون دور[1] و با اعمال محدودیت زمانی استراتژی حمله را نمایش می‌دهند. در این گراف، گره‌ها حمله و یال‌ها ترتیب زمانی بین حملات را نشان می‌دهند.

۳-۷-۲-اولویت‌دهی به هشدارها: سامانه‌های تشخیص نفوذ در طول روز حجم عظیمی از هشدارها را تولید می‌کنند. در میان این هشدارها، هشدارهای مثبت اشتباه و نامرتبط نیز وجود دارد. برخی هشدارهای صحیحی که تولید می‌شوند، ممکن است نسبت به برخی دیگر کم‌اهمیت‌تر باشند. به همین منظور بهتر است، هشدارهای مهم‌تر را از سایرین جدا کنیم. در [۴۳] براساس مشخصات و پیکربندی سامانه و میزان اهمیتی که آن سامانه دارد با استفاده از فرمولی میزان اهمیت هر هشدار را محاسبه می‌کند. Lippmann در [۴۵] تنها براساس آسیب‌پذیری‌های یک سامانه به اولویت‌دهی هشدارهای آن پرداخته است.

۳-۷-۳-تحلیل تأثیر: تحلیل تأثیر امکان برقراری ارتباط بین خرابی یک سرویس در شبکه و حملات انجام‌شده به آن شبکه را فراهم می‌کند. در [۶] تحلیل تأثیر با استفاده از هشدارها، یک پایگاه داده و ارسال یک‌سری سیگنال انجام می‌شود. در پایگاه داده سرویس‌های نصب‌شده، اطلاعات وابستگی بین این سرویس‌ها و میزان اهمیت آن‌ها برای عملیات کلی شبکه درج شده است. هنگامی‌که هشداری حمله به یک سرویس را گزارش می‌کند، در این پایگاه داده تأثیر آن سرویس بر سایر سرویس‌ها بررسی شده و با ارسال سیگنال‌های ضربان قلب[2] در حال اجرابودن سرویس‌های وابسته بررسی می‌شود.

۴-تشریح فرآیند همبسته‌سازی هشدار در OSSIM

پژوهش‌های صورت‌گرفته در زمینهٔ همبسته‌سازی هشدار در بخش ۳ مرور شد. با بررسی عملکرد سامانهٔ OSSIM و امکاناتی که ارائه می‌کند، مؤلفه‌های موجود در سامانهٔ OSSIM را براساس مدل ارائه‌شده توسط والوئر در بخش ۳، و پژوهش‌هایی که در ادامهٔ آن بیان شد، استخراج کردیم و نتیجه را در ادامه بیان می‌کنیم. این سامانه تنها برخی از مؤلفه‌های همبسته‌سازی را دارد، در مقایسه با مؤلفه‌های مطرح در [۶] دارای مؤلفه‌های زیر است:

۴-۱-هنجارسازی(۳-۱-۱[3]): هنجارسازی در سامانهٔ OSSIM ، در دو بخش صورت می‌گیرد.

- روی عامل‌ها، توسط پلاگین‌ها: عامل‌ها هشدارها را متناسب با فیلدهایی که در پلاگین تعریف‌شده، هنجارسازی کرده و به سرور ارسال می‌کنند. در این سامانه به‌دلیل اینکه از هشدارهای متنوع که متعلق به دسته‌های تشخیص و جلوگیری از نفوذ و رفتارهای مخرب هستند، بهره‌برداری می‌شود، نمی‌توان قالب استاندارد رایج IDMEF را به آن‌ها اعمال کرد.

روی سرور: OSSIM برای همبسته‌سازی، به فیلدهایی فراتر ازآنچه عامل‌ها ارائه می‌کنند، نیاز دارد؛ بنابراین چند فیلد در پلاگین‌ها به هشدارها اضافه می‌شود که این فیلدها بعدها توسط سرور مقداردهی می‌شوند [۳].

۴-۲-پیش‌پردازش(۳-۱-۲): هنگام دریافت هشدارها توسط سامانهٔ OSSIM درصورتی‌که فیلدهای مورد نیاز همبسته‌سازی مقداری نداشته باشند، به آن‌ها به‌صورت پیش‌فرض مقداری را تخصیص می‌دهد. به‌عنوان مثال درصورت خالی‌بودن مقدار درگاه، مقدار پیش‌فرض صفر را به آن تخصیص می‌دهد.

۴-۳-تأیید هشدار(۳-۱-۴): در این سامانه از چند منبع داده برای همبسته‌سازی هشدار استفاده می‌شود. منابع دادهٔ مورد استفاده عبارت‌اند از:

- پایگاه دادهٔ آسیب‌پذیری
- فهرست دارایی‌های سازمان
- پایگاه دادهٔ هشدارها

استفاده از چند منبع بالا، سبب شده است که با تأیید هشدارها تعداد هشدارهای مثبت اشتباه را کاهش دهد. این نوع تأیید را در قالب هبسته‌سازی تقاطعی و دارایی در بخش مربوط به همبسته‌سازی هشدار بیان می‌کنیم.

[1] Direct Acyclic Graph
[2] Heartbeat

[3] شماره گذاری‌های درون پرانتز به مؤلفه‌های مدل والوئر اشاره می‌کنند، به این معنی که این مؤلفه از مدل والوئر در سامانه OSSIM وجود دارد. اما نحوهٔ انجام کار آنها لزوماً یکسان نیست.

۴-۴-تشخیص کانون حمله(۳-۱-۷): در این سامانه می‌توان با تعریف قوانین حملات یک‌به‌چند و چندبه‌یک را شناسایی کرد. به این صورت که اگر نشانی مقصد هشدارهای زیادی ثابت و نشانی مبدأ آن‌ها متفاوت بود، حمله چندبه‌یک و درصورتی‌که نشانی مبدأ هشدارهای زیادی با نشانی‌های مقصد متفاوت یکی بود، حمله یک‌به-چند تشخیص داده می‌شود. نوع حمله در این هشدارها باید یکسان در نظر گرفته شود. نحوهٔ تعریف قوانین در ادامه بیان می‌شود.

۴-۵-همبسته‌سازی(۳-۱-۸): یکی از مهم‌ترین عملیاتی که سامانهٔ OSSIM انجام می‌دهد همبسته‌سازی هشدار است، که منجر به کاهش تعداد هشدارها و هشدارهای مثبت اشتباه می‌شود. همبسته‌سازی هشدارها متناسب با نوع هشدار و اطلاعاتی راجع به مقصد آن به سه روش زیر انجام می‌شود:

- همبسته‌سازی منطقی: همبسته‌سازی هشدارهای متفاوت
- همبسته‌سازی تقاطعی: همبسته‌سازی هشدارها و آسیب‌پذیری‌ها
- همبسته‌سازی دارایی: همبسته‌سازی هشدارها با استفاده از سرویس‌ها و سیستم‌عامل

همبسته‌سازی نوع دوم و سوم تنها هشدار را تأیید می‌کنند. اما نوع نخست بیش از یک هشدار را می‌تواند همبسته کند. در ادامه سه نوع همبسته‌سازی را تشریح می‌کنیم:

۴-۵-۱-همبسته‌سازی منطقی

این نوع همبسته‌سازی بیش از یک هشدار را همبسته می‌کند. براساس همبسته‌سازی مبتنی بر سناریوهای حملهٔ ازپیش‌تعریف‌شده، عمل می‌کند. سناریوی حملات توسط فرد خبره استخراج و با تعریف قوانین همبسته‌سازی، این سناریو بیان می‌شود و برای همبسته‌سازی هشدارها مورد استفاده قرار می‌گیرد. برای هر حمله یک راهنما[1] نوشته می‌شود که از چند سطح قانون تشکیل‌شده است. هر سطح قانون مستقل از سایر سطوح است و مشخصات مربوط به خود را دارد. تمام هشدارهایی که برای تشخیص یک حمله ضروری‌اند باید در سطوح راهنمای آن حمله در نظر گرفته شوند. یک نمونه راهنما برای تشخیص حمله Bruteforce در ادامه آورده شده است:

```
<directive id="500001" name="Bruteforce SSH Authentication Attack" priority="5">
  <rule type="detector" name="ssh authentication failure" from="ANY" to="79174bd2-3ecb-a5c3-2850-3ee5e0bd18a2" port_from="ANY" port_to="ANY" reliability="5" occurrence="5" plugin_id="4003" plugin_sid="1,2,3,4,5,6,12,13,14">
  <rules>
        <rule type="detector" name="ssh authentication failure 5 times" from="1:SRC_IP" to="1:DST_IP" port_from="1:SRC_PORT" port_to="1:DST_PORT" reliability="10" occurrence="5" time_out="120" plugin_id="4003" plugin_sid="1:PLUGIN_SID" protocol="1:PROTOCOL" sensor="1:SENSOR"/>
</rules>
</rule>
</directive>
```

در این راهنما دو سطح قانون نوشته شده است. با پنج‌بار دریافت، هشداری به نام "ssh authentication failure" قانون سطح نخست کامل شده و به سطح دوم می‌رود. درصورتی‌که پنج هشدار در بازهٔ زمانی ۱۲۰ ثانیه بعد از آخرین هشدار دریافت شود، سطح دوم هم کامل شده و یک هشدار سطح بالا با بالاترین میزان ریسک و قابلیت اطمینان تولید می‌شود. هنگامی‌که یک هشدار با قانون سطح نخست یک راهنما مطابقت می‌کند، به‌دلیل اینکه با احتمال زیاد هشدار مربوط به سطح دوم آن به‌زودی دریافت می‌شود، آن راهنما در بخشی از حافظه مقیم می‌شود. موتور همبسته‌سازی با دریافت یک هشدار، ابتدا تمام فیلدهای آن را با راهنماهای مقیم در این بخش حافظه مقایسه کرده و درصورتی‌که مطابقت حاصل نشود، هشدار را با نخستین قانون از راهنماها مقایسه می‌کند، تا زمانی که با یکی از راهنماها مطابقت کند؛ سپس آن راهنما را در حافظه قرار می‌دهد و به همین ترتیب کار را ادامه می‌دهد. با تطبیق آخرین قانون از یک راهنما، هشداری سطح بالاتر و با قابلیت اطمینان بیشتر صادر می‌شود.

۴-۵-۲-همبسته‌سازی تقاطعی

OSSIM در جدولی اطلاعاتی راجع به هر سیستم درون محدوده نظارتی خود را ذخیره می‌کند. این اطلاعات در سه دسته زیر جای می‌گیرند:

- آسیب‌پذیری‌ها

[1] Directive

- سیستم‌عامل
- درگاه‌های باز

هنگامی‌که با استفاده از پویش‌گران آسیب‌پذیری و شبکه، سیستم‌ها پویش می‌شوند، اطلاعات مربوط به آسیب‌پذیری و مشخصات آن‌ها به همراه نشانی IP آن‌ها در جدولی ذخیره می‌شود. همبسته‌سازی تقاطعی، با بررسی هشدار دریافتی از سامانهٔ تشخیص نفوذ و مقایسه با آسیب‌پذیری‌های تشخیص داده‌شده توسط پویش‌گر آسیب‌پذیری، درصورتی‌که سیستم هدف، نسبت به حمله تشخیص داده‌شده در هشدار آسیب‌پذیر باشد، اولویت هشدار را زیاد می‌کند. این نوع از همبسته‌سازی به پایگاه داده آسیب‌پذیری و جدول همبسته‌ساز تقاطعی تشخیص‌دهنده بستگی دارد . OSSIM از پایگاه داده آسیب‌پذیری OSVDB و جدول همبسته‌ساز تقاطعی Nessus و Snort NIDS استفاده می‌کند[۳،۲].

۴-۵-۳- همبسته‌سازی دارایی

با توجه به اینکه هر حمله بر روی یک سرویس یا سیستم‌عامل خاص مؤثر است، این روش همبسته‌سازی بررسی می‌کند که آیا سیستمی که حمله روی آن گزارش‌شده این سرویس یا سیستم‌عامل را دارد یا خیر. درصورتی‌که وجود نداشته باشد، آن را مثبت اشتباه قلمداد می‌کند. این نوع همبسته‌سازی بستگی به میزان صحت فهرست سرویس‌ها و سایر ویژگی‌های سیستم‌ها دارد. OSSIM از جمع‌آوری این اطلاعات به‌صورت خودکار و دستی پشتیبانی می‌کند. روش‌های همبسته‌سازی تقاطعی و دارایی فقط هشدارها را تأیید می‌کنند و دو یا چند هشدار را با یکدیگر همبسته نمی‌کنند[۳،۲] .

۴-۶-اولویت‌دهی(۳-۱-۱۰): در سامانهٔ OSSIM به دو صورت به هشدارها اولویت تخصیص می‌یابد.

- اگر هشدار با یک سیاست مطابقت داشته باشد، مقدار مشخص‌شده در آن سیاست به‌عنوان اولویت به آن تخصیص می‌یابد.
- در غیر این صورت پس از دریافت هر هشدار براساس امضای آن هشدار، اولویتی به آن منتسب می‌شود. در پایگاه داده OSSIM به هرکدام از امضاهای پلاگین‌ها اولویتی تخصیص داده شده است.

۴-۷-معماری

این سامانه به دو صورت متمرکز و سلسله‌مراتبی می‌تواند هشدارها را مدیریت کند. در حالت متمرکز تمام عملیات را سرور مرکزی انجام می‌دهد.

۵-نتیجه‌گیری و کارهای آینده

در این مقاله با یک رویکرد ترکیبی، مسألهٔ همبسته‌سازی هشدار و تشخیص حملات چندگامی بررسی شد. ابتدا سامانهٔ OSSIM معرفی شد، سپس فرآیند همبسته‌سازی تشریح و کارهای صورت گرفته در این زمینه بررسی شدند. با دید مقایسه‌ای نسبت به پژوهش‌های صورت‌گرفته در زمینهٔ دانشگاهی و نتایج حاصل از پیاده‌سازی و استفاده از این سامانه در محیط آزمایشگاهی و محیط واقعی، فرآیند همبسته‌سازی هشدار در سامانهٔ OSSIM را تشریح کردیم. سامانهٔ OSSIM ، قابلیت‌ها و نقاط ضعفی دارد که در ادامه آورده شده‌اند. این سامانه قابلیت‌هایی را با یک‌پارچه‌سازی ابزارهای امنیتی و نظارتی متن‌باز و تجاری فراهم کرده است؛ ازجملهٔ این قابلیت‌ها می‌توان موارد زیر را نام برد:

- تشخیص سطح پایین و بلادرنگ تهدیدات شناخته‌شده و فعالیت‌های غیرعادی (حملات شناخته‌نشده)
- انجام وظیفه به‌صورت خودکار[1]
- ممیزی شبکه، میزبان‌ها و سیاست‌های امنیتی
- آنالیز رفتار شبکه به‌صورت کلی و در وضعیت‌های خاص
- مدیریت هشدارها
- هوشمندی که دقت تشخیص تهدیدها را افزایش می‌دهد.
- تحلیل امنیتی مبتنی بر ریسک
- گزارش‌های اجرایی و فنی
- دارای معماری با کارایی بالا و قابل‌افزایش

در کنار قابلیت‌های بیان‌شده این سامانه دارای نقاط ضعفی نیز هست، که ازجمله آن‌ها می‌توان به موارد زیر اشاره کرد:

- مستندسازی ضعیف
- تکرار هشدارهای مشابه
- درنظرگرفتن پنجرهٔ زمانی
- همبسته‌سازی حملات براساس الگو

[1] Compliance Automation

- هشدارهای متنوع را دریافت می‌کند، اما آن‌ها را با یکدیگر همبسته نمی‌کند.

برای بهبود این سامانه، در زمینه همبسته‌سازی، حملاتی که از پیش، الگویی برای آن‌ها تعریف نشده است و همین‌طور استفاده از تمام قابلیت‌هایی که با جمع‌آوری هشدارهای متنوع می‌تواند فراهم شود، موارد زیر پیشنهاد می‌شود:

- بهبود روش همبسته‌سازی هشدار و خودکارسازی آن
- استفاده از هشدارهای تمام منابع داده در همبسته‌سازی
- تغییر قالب هشدارها درصورت استفاده از سایر هشدارها حذف تکرار هشدارها
- کاهش تأثیر زمان انجام حمله (پنجره زمانی)
- حذف هشدارهای نامرتبط
- افزودن هشدارهای منفی اشتباه
- پیش‌بینی حمله
- اضافه‌کردن پلاگین برای منابع داده دیگر

۶- مراجع:

[1] Alienvault Group, 2010, AlienVault SIEM Sy-tem Description [Online]. Available FTP: do cs.h-uihoo.com/ossim/av-siem-system-descrip tion-v4.pdf

[2] J. Blasco, D. Karg, (2011, September), Advanced attack detection using OSSIM (Onl-ne),Availa ble:http://www.alienvault.com /blog-conten t/2011/09/Advanced_attack_detection_using_OS SIM.pdf

[3]Alienvault Group, (2003,November), OSSIM General System Description (Online), Availabl e:https://www.alienvault.com/docs/OSSIM-desc-en.pdf

[4]Alienvault Group, AlienVault_Users_Man ual_1.0(Online),Available: https://scadahacker. com /library/Documents/Manuals/AlienVault _Users_Manual_1.0.pdf

[5] DR. MILLER, Sh. HARRIS, AA. HARPER, S. VANDYKE, Ch. BLASK, Security Informa tion and Event Management (SIEM) Implement ation, ch 7,8, 2011 by The McGraw-Hill Com panies

[6] F. Valeur, G. Vigna, C. Kruegel, R.A. Kemm erer, A comprehensive approach to intrusion detec-tion alert correlation, dependable and sec ure computing, Journal of IEEE Transactions 1 (2004) 146–169.

[7] D. Curry and H. Debar, "Intrusion Detection Message Exchange Format: Extensib le Markup Language (XML) Document Type Definition," draft-ietf-idwg-idmef-xml-10.txt+, Jan. 2003.

[8] M. Walker, CEH Certified Ethical Hacker, McGraw-Hill Companies, 2011

[9] A. E. Taha, I. Abdel Ghaffar, A. M. Bahaa Eldin and H. M. K. Mahdi, "Agent Based Correlation Mo-del For Intrusion Detection Alerts," Publi shed by the IEEE Computer Society, May 2010.

[10]H.T. Elshoush, I. M. Osman, An Improved Fram ework for Intrusion Alert Correlation, Proce-edings of the World Congress on Engi neering 2012 Volume I;2012, p518.

[11] J. Yu, Y.V.R. Reddy, S. Selliah, S. Kanka nahalli, S. Reddy, V. Bharadwaj, TRINETR: An intrusion detection alert management systems, in: Proc. of 13th IEEE Int. Workshops on Enabling Technologies:Infrastructure for Collab orative Enterprises (WET ICE), 2004, pp. 235–240.

[12]A.A. Mohamed, O. Basir, Fusion based app roach for distributed alarm correlation in com puter networks, in: Proc. of the 2nd Int. Conf. on Communication Software and Networks (ICCSN '10), 2010, pp. 318–324.

[13]R. Khatoun, G. Doyen, D.R. Saad, A. Serhr ouchni, Decentralized alerts correlation approach for DDoS intrusion detection, in: Proc. of the Int. Conf. on New Technologies, Mobility and Security (NTMS '08), 2008, pp. 1–5.

[14]S. Salah, G. Macia-Fernandez, J.E. E. Diaz-Verdejo, A model-based survey of alert corre lation techniques, ELSEVIER Computer Net works 57 (2013) 1289–1317.

[15]T. Donghai, C. Hu, Q. Yang, J. Wang, Hiera rchical distributed alert correlation model, in: Proc. of the 5th Int. Conf. on Information Assu rance and Security(IAS'09), 2009, pp. 765–768.

[16]R. Costa, N. Cachulo, P. Cortez, An intelligent alarm management system for large-scale telec om-munication companies, in: Proc. of the 14th Portuguese Conf. on Artificial Intelli gence (EPIA'09), 2009, pp. 386–399.

[17]Y. Chen, J. Lee, Autonomous mining for alarm correlation patterns based on time-shift similarity clustering in manufacturing system, in: Proc. of the Int. Conf. on Prognostics and Health Management (PHM'11), 2011, pp. 1–8

[18]X. Zhuang, D. Xiao, X. Liu, Y. Zhang, Ap-plying data fusion in collaborative alerts corr-lati on, in: Proc. of the Int. Symposium of Computer Science and Computational Technology (ISC SCT '08), vol. 2, 2008, pp. 124–127.

[19] J. Chang, J. Yu, Y. Pei, MS2IFS: a multiple source-based security information fusion system, in: Proc. Of the Int. Conf. on Communications and Intelli-gence Information Security (ICC IIS'10), 2010, pp. 215–219.

[20] C. Abad et al., "Log Correlation for Intrusion Detection: A Proof of Concept," Proc. 19th Ann. Computer Security Applications Conference, IEEE CS, 2003, pp. 255–246.

[21]Sh. Davidoff , J. Ham , "Network Forensics, " in Tracking Hackers through Cyberspace, first Ed. New Jersey : prentice hall, 2012, ch. 8, Sec. 1, pp. 291-305.

[22] A. A. Chuvakin, K. J. Schmidt, Ch. Phillips, "Logging and Log Management," The Aut horitative Guide to Understanding the Concepts Surrounding Logging and Log Management, first Ed. Massachusetts : Syngress, 2013, ch. 3, pp. 114-135.

[23] A. Valdes and K. Skinner, "Probabilisc Alert Correlation," pp. 54-68, 2001

[24] F. Cuppens, Managing alerts in a multi-intru sion detection environment, in: Proc. of the 17th Annual Conf. on Computer Security Applications, 2001, pp. 22–31.

[25] A. Siraj, R.B. Vaughn, Multi-level alert clustering for intrusion detection sensor data, in: Proc. of the Annual Meeting of the North Ame rican Fuzzy Information Processing Society (NAFIPS), 2005, pp. 748–753.

[26] K. Julisch, Clustering intrusion detection alarms to support root cause analysis, Journal of ACM Transaction on Information System Securi ty 6 (2003) 443–471.

[27] K. Julisch, M. Dacier, Mining intrusion detec tion alarms for actionable knowledge, in: Proc. of the 8th ACM Int. Conf. on Knowledge Discovery and Data Mining, 2002, pp. 366–375.

[28] H. Debar, A. Wespi, Aggregation and correla-tion of intrusion–detection alerts, in: Proc. of the Int. Symposium on Recent Advances in Intrusion Detection (RAID'02), 2002, pp. 85–103.

[29] S.H. Ahmadinejad, S. Jalili, Alert correl ation using correlation probability estimation and time windows, in: Proc. of the Int. Conf. on Co-mputer Technology and Development (ICC-TD'09), vol. 2, 2009, pp. 170–175.

[30] J. Ma, Z. Li, W. Li, Real-time alert stream clustering and correlation for discovering stra tegies, in: Proc. of the Int. Conf. on Fuzzy Systems and Knowledge Discovery (FSKD'08), vol. 4, 2008, pp. 379–384.

[31] X. Qin, W. Lee, Statistical causality analy sis of infosec alert data, in: Proc. of the 6th Int. Symposium on Recent Advances in Intrusion Detection (RAID'03), 2003, pp. 73–93.

[32] B. Morin, H. Debar, Correlation of intrus ion symptoms: an application of chronicles, in: Proc. of the 6th Int. Conf. on Recent Advances in Intrusion Detection (RAID'03), 2003, pp. 94–112.

[33] Ning, P., Xu, D.: Adapting Query Optimiz ation Techniques for Efficient Intrusion Alert Corr-elation. Technical Report TR-2002-14 NCS U Dept. of Computer Science (2002).

[34] Lin Zhaowen; Li Shan; Ma Yan, "Real-Time Intrusion Alert Correlation System Based on Prerequisites and Consequence," Wireless Communications Networking and Mobile Computing (WiCOM), 2010 6th International Conference on , vol., no., pp.1,5, 23-25 Sept. 2010.

[35] P. Ning, Y. Cui, D. Reeves, D. Xu, Techniq ues and tools for analyzing intrusion alerts, Journal of ACM Transactions on Information and System Security 7 (2004) 274–318.

[36] Jingmin Zhou , Mark Heckman , Brennen Reyno-lds , Adam Carlson , Matt Bishop, Modeli ng network intrusion detection alerts for correla tion, ACM Transactions on Information and Syst em Security (TISSEC), v.10 n.1, p.4-es, February 2007 [doi>10.1145/1210263. 1210 267].

[37] Sherif Saad, Issa Traore, Semantic aware attack scenarios reconstruction, Journal of Information Security and Applications, Volume 18, Issue 1, July 2013, Pages 53-67, ISSN 2214-2126, http://dx-.doi.org/10.1016/j.jisa .2013 .08.002.

[38] F. Alserhani, M. Akhlaq, I. Awan, A. Cull en, MARS: multi-stage attack recognition system, in: Proc. of the 24th IEEE Int. Conf. on Advanced Information Networking and Applic ations (IFIP-/IEEE), 2010, pp. 753–759.

[39] S. Templeton, K. Levitt, A requires/provid es model for computer attacks, in: Proc. of the Int. Workshop on New Security Paradigms (NSP W), 2000, pp. 31–38.

[40] S. Xiao, Y. Zhang, X. Liu, J. Gao, Alert Fusion Based on Cluster and Correlation Analysis, in: Proc. of the Int. Conf. on Convergence and Hybri d Information Technol ogy (ICHIT'08),(2008) 163-68.

[41] S.T. Eckmann, G. Vigna, and R.A. Kemme rer, Statl: An attack language for state-based intrusion detection, Proceedings of the 1st ACM Workshop on Intrusion Detection Systems (Athens, Greece), November 2000.

[42] O.M. Dain and R. K Cunningham, Fusing a heterogeneous alert stream into scenarios, Proceedings of the 2001 ACMWorkshop on Data Mining for Security Applications, 2001, pp. 1–13.

[43] P. Porras, M. Fong, and A. Valdes, "A Mission-Impact-Based Approach to INFOSEC Alarm Correlation," Proc. Int'l Symp. The Recent Advances in Intrusion Detection, pp. 95-114, Oct. 2002

[44] Peng Ning, Yun Cui, and Douglas S. Reeves, Constructing attack scenarios through correlation of intrusion alerts, Proceedings of the 9th ACM conference on Computer and communication security (Washington D.C., USA), ACM Press, November 2002, pp. 245–254.

[45] Richard Lippmann, Seth Webster, and Douglas Stetson, The effect of identifying vulnerabilities and patching software on the utility of network intrusion detection, Proceedings of Recent Advances in Intrusion Detection, 5th International Symposium, (RAID 2002) (Zurich, Switzerland) (A. Wespi, G. Vigna, and L. Deri, eds.), Lecture Notes in Computer Science, Springer-Verlag Heidelberg, October 2002, pp. 307–326.

مهدیه صفرزاده واحد، فارغ‌التحصیل کارشناسی ارشد رشته فناوری ارتباطات و اطلاعات گرایش امنیت اطلاعات از دانشگاه صنعتی مالک اشتر در سال ۹۳ و کارشناسی علوم کامپیوتر از دانشگاه تبریز است. زمینه‌های پژوهشی ایشان امنیت شبکه، مرکز عملیات امنیت و همبسته‌سازی هشدارها برای استخراج سناریوی حملات است.

علیرضا نوروزی مدرک کارشناسی را در رشته مهندسی کامپیوتر (نرمافزار) از دانشگاه فردوسی مشهد اخذ کرده است؛ سپس دوره کارشناسی ارشد خود را در رشته علوم کامپیوتر در دانشگاه صنعتی شریف به اتمام رساند. وی مدرک دکترای خود را در رشته علوم کامپیوتر از دانشگاه صنعتی امیرکبیر اخذ کرده است. ایشان در حال حاضر، استادیار دانشگاه صنعتی مالک اشتر بوده و در پژوهشکده امنیت، عضو هیأت علمی گروه علمی امنیت اطلاعات و ارتباطات است. زمینه‌های پژوهشی مورد علاقه ایشان موضوعات امنیت شبکه، حملات سایبری، ارزیابی امنیتی، فرماندهی و کنترل، و مدیریت بحران است.

محمد امین عراقی زاده مدرک کارشناسی سخت‌افزار کامپیوتر را از دانشگاه ازاد اسلامی واحد تهران مرکزی در سال ۸۶ و کارشناسی ارشد معماری کامپیوتر را از دانشگاه اصفهان در سال ۸۸ اخذ کرده است. وی هم‌اکنون دانشجوی دکترای معماری کامپیوتر در دانشگاه تهران است. زمینه پژوهشی مورد علاقه ایشان امنیت شبکه های کامپیوتری است.