مدلی امنیتی نوینی برای ارزیابی خطر حملات چند مرحله ای در شبکه های کامپیوتری

مرجان کرامتی[1]

۱- مربی- دانشکده ریاضی، آمار و علوم کامپیوتر- دانشگاه سمنان- سمنان- ایران

keramati_marjan@semnan.ac.ir

چکیده: اندازه‌گیری و مدیریت خطر متناظر با حملات، همواره یکی از چالش‌برانگیزترین مشکلاتی است که برای مدیریت امنیت شبکه یک سازمان وجود داشته است. مدیریت خطر حملات تنها با ارزیابی آسیب‌پذیری‌های موجود ممکن خواهد بود. اولویت‌بندی آسیب‌پذیری‌ها به مدیران امنیتی این امکان را می‌دهد تا درک مناسبی از زیرساخت داشته باشند و بدین ترتیب پرخطرترین حملات را مشخص و با توجه به محدودیت هزینه در هر سازمان، هزینه تنها برای برطرف‌سازی حملات پرخطر صرف شود.در حال حاضر اکثر حملات موجود در شبکه‌های کامپیوتری، حملات چند مرحله‌ای هستند که در آنها مهاجم با بهره‌برداری از چندین آسیب‌پذیری با ترتیب مشخص می‌تواند به نقطه مورد نظر خود حمله کند. بنابراین در نظر گرفتن ارتباطات بین آسیب پذیری‌ها به منظور ارزیابی خطر حملات، اجتناب‌ناپذیر است. چالش بزرگی که در ارزیابی خطر حملات از نقطه نظر برآورد خطر حملات چندمرحله‌ای وجود دارد این است که اکنون، هیچ مرجعی برای یافتن ارتباط بین سیل عظیم آسیب‌پذیری‌های موجود در سیستم‌های کامپیوتری وجود ندارد و ارزیابی خطر تنها برای حملات تک مرحله ای انجام می‌شود. در این مقاله یک مدل امنیتی برای ارزیابی خطر حملات چند مرحله ای پیشنهاد شده است که دقت و صحت ارزیابی خطر را نسبت به سیستم های ارزیابی خطر موجود بهبود می بخشد.

واژه‌های کلیدی: آسیب پذیری، ارزیابی خطر، حمله چند مرحله‌ای، الگوی حمله، معیار امنیتی

نوع مقاله: پژوهشی

DOI: 10.29252/jiaeee.18.3.1189

تاریخ ارسال مقاله: ۱۳۹۹/۶/۳۰

تاریه پذیرش مشروط مقاله: ۱۳۹۹/۱۰/۲۱

تاریخ پذیرش مقاله: ۱۴۰۰/۲/۱۱

نام نویسنده‌ی مسئول: مرجان کرامتی

نشانی نویسنده‌ی مسئول: ایران – سمنان – کیلومتر ۵ جاده دامغان – دانشگاه سمنان – دانشکده ریاضی، آمار و علوم کامپیوتر

۱- مقدمه

مدیریت کارای خطر به‌منظور بقای عملیات تجاری و انجام ماموریت های سازمانی امری ضروری به‌نظر می‌رسد. افزایش سیستم‌ها، شبکه‌ها، برنامه‌های کاربردی، ابزارهای سیار و تمایل به سمت و سوی مجازی سازی و محاسبات ابری، می‌تواند محیطی ایجاد کند که، نرخ بروز حملات در آن سیر روزافزونی دارد. از اطلاعات محرمانه تجاری و اختصاصی گرفته تا گزارشات حساس پزشکی به دلیل جریان‌های داده مهمی که در این سیستم‌ها وجود دارد در معرض حملات قرار دارند. یک نقص امنیتی، ممکن است نتیجه یک خطای ناخواسته توسط کاربر مجاز باشد، یا توسط تعداد قابل‌توجهی از سازمان‌هایی انجام شود که هدفشان سرقت اطلاعات تجاری یا شخصی مشتریان سازمان یا خرابی های تبهکارانه‌ای با اهداف سیاسی باشد. یک رخنه امنیتی، می‌تواند شماره کارت اعتباری تعدادی از مشتریان را از روی پایگاه داده حذف نماید، یک شبکه برق را قطع کند و یا صدمات جبران‌ناپذیر سیاسی و اقتصادی برای یک کشور به‌همراه داشته باشد.

منابع هر سازمان محدود هستند، با این وجود تعداد آسیب‌پذیری‌های شناخته شده عموما آنقدر زیاد هستند که برطرف کردن کامل آنها غیر ممکن خواهد بود. شبکه‌ای را در نظر بگیرید که، شامل ده‌ها هزار میزبان است که هز کدام به‌شکل متوسط شامل ۱۰ یا ۲۰ عدد آسیب پذیری هستند بنابراین صدها هزار آسیب‌پذیری در سازمان وجود خواهند داشت. آسیب‌پذیری‌های سخت‌افزاری و نرم‌افزاری برای سازمان‌هایی که برمبنای شبکه‌های کامپیوتری عمل می‌کنند خطر جدی به شمار می‌آید و طبقه‌بندی و برطرف‌سازی آن‌ها امر دشواری است. عملکرد ابزارهای مدیریت آسیب‌پذیری سنتی به این صورت است که، یک لیست از نقاط ضعف شناسایی شده که به صورت کیفی رده‌بندی شده‌اند (برای مثال سطوح متوسط، پایین بالا یا یک تا پنج) را ارائه می‌دهند. واضح است که، صرفاً لیست کردن خطرات موجود در شبکه کافی نخواهد بود. سازمان باید یک مجموعه معیار در اختیار داشته باشد تا، توسط آنها آسیب‌پذیری‌های شناسایی شده در سازمان را رتبه‌بندی کند و به صورت کارا تصمیماتی را به‌منظور کاهش میزان خطر در سازمان اتخاذ نماید. به عبارت دیگر، نیازمند یک مدل برای تحلیل خطر آسیب‌پذیری‌های هر شبکه هستیم.

در مبحث امنیت شبکه، آسیب‌پذیری یک نقطه ضعف در طراحی یا یک اشکال در پیاده‌سازی است که می‌تواند منجر به نقض پارامترهای امنیتی محرمانگی، یکپارچگی یا دسترسی‌پذیری داده‌ها در یک شبکه شود. منظور از ارزیابی یک آسیب‌پذیری، فرآیند تشخیص، کمی‌سازی و اولویت‌بندی آسیب‌پذیری‌ها در یک سیستم است. اولویت‌بندی آسیب‌پذیری‌ها به مدیران امنیتی این امکان را می‌دهد تا درک مناسبی از زیرساخت سازمان خود داشته باشند و بدین ترتیب پرخطرترین حملات را مشخص و با توجه به محدودیت هزینه در هر سازمان، هزینه تنها برای برطرف‌سازی حملات پرخطر صرف شود.

ارزیابی خطر یک آسیب‌پذیری نیازمند تخمین میزان احتمال بهره برداری از آسیب‌پذیری و تعیین آثار مخرب ناشی از بهره‌برداری از آن روی پارامترهای امنیتی از جمله محرمانگی، یکپارچگی و دسترسی پذیری است. برای این‌منظور باید تعدادی معیار امنیتی در اختیار داشته باشیم که بتوانند به‌شکل کمی اندازه‌گیری شوند.

در حال حاضر اکثر حملات موجود در شبکه‌های کامپیوتری، حملات چند مرحله‌ای هستند که در آنها مهاجم با بهره‌برداری از چندین آسیب‌پذیری با ترتیب مشخص می‌تواند به نقطه مورد نظر خود حمله کند. بنابراین در نظر گرفتن ارتباطات بین آسیب‌پذیری‌ها به‌منظور ارزیابی دقیق حملات، مسئله‌ای اجتناب‌ناپذیر است. سیستم‌های موجود امتیاز دهی را تنها برای تک آسیب‌پذیری و بدون در نظر گرفتن وابستگی آن به سایر آسیب‌پذیری‌ها در شبکه انجام می‌دهند، بنابراین ارزیابی صحیحی از میزان خطر یک آسیب‌پذیری نخواهند داشت.

از طرفی، فقدان گوناگونی امتیازات محاسبه شده با استفاده از سیستم های موجود (مانند CVSS) برای ارزیابی خطر آسیب پذیری ها برای رتبه‌بندی سیل عظیمی از آسیب‌پذیری‌ها. چالشی جدی به شمار می آید

حملاتی که آسیب‌پذیری‌های موجود را برای نقض سیاست‌های امنیتی استفاده می‌کنند ممکن است توسط یک حمله واحد یا دنباله‌ای از حملات تک‌مرحله‌ای انجام شوند. به دنباله حملات تک‌مرحله‌ای گاهاً زنجیره بهره‌برداری نیز گفته می‌شود. زنجیره بهره‌برداری، از وابستگی های موجود بین آسیب‌پذیری‌ها به‌عنوان ابزاری برای مختل کردن سیاست‌های امنیتی استفاده می‌کند [۱].

مجموعه تمامی زنجیره‌های بهره‌برداری که سیاست‌های امنیتی را نقض می‌کنند می‌توانند توسط یک گراف حمله مشخص شوند. شماری از اطلاعات امنیتی یک شبکه با تجزیه و تحلیل گراف حمله آن قابل استخراج است. چرا که، گراف حمله نمایش خلاصه‌ای از تمامی راه های ممکن برای نفوذ به شبکه و مختل کردن سیاست‌های امنیتی است. گراف حمله به‌عنوان یک ابزار ارزیابی آسیب‌پذیری می‌تواند به یک سازمان کمک کند که وضعیت امنیتی خود را مشخص سازد. یک سازمان می‌تواند از گراف حمله برای تعیین چگونگی نفوذ مهاجم به شبکه استفاده کند. بر اساس مسیرهای مشخص شده، یک سازمان قادر خواهد بود راهکارهایی را برای کاهش خطر پیشنهاد دهد. اگر یک مهندس امنیتی از معیارهای امنیتی مبتنی بر گراف حمله استفاده کند، می‌تواند یک استراتژی را برای انتخاب اقدامات متقابل بکارگیرد یا امنیت دو پیکره‌بندی متفاوت از شبکه مورد نظر را با هم مقایسه کند. زمانی که گراف حمله در کنار معیارهای امنیتی مبتنی بر گراف حمله استفاده می‌شود، می‌تواند برای ارزیابی کمی شماری از جنبه‌های امنیتی شبکه استفاده شود [۱].

اما نکته ای که وجود دارد این است که، گراف حمله یک سیستم کامپیوتری لزوماً در دسترس نیست و یک سیستم امتیازدهی باید قادر

باشد مستقل از گراف حمله آن سیستم، ارزیابی خطر حملات چندمرحله ای را انجام دهد. به بیان دیگر، یک سیستم امتیازدهی باید قادر باشد ارزیابی خطر یک آسیب‌پذیری را با در نظر گرفتن چگونگی ارتباط آن با سایر آسیب‌پذیری ها انجام دهد. بدین معنا که، بهره برداری شدن از یک آسیب پذیری نیازمند بهره برداری از چه آسیب‌پذیری‌هایی است و بهره برداری از این آسیب‌پذیری منجر به بالفعل شدن کدام آسیب‌پذیری‌ها می شود.

سیستم‌های موجود امتیاز دهی را تنها برای تک آسیب‌پذیری و بدون در نظر گرفتن وابستگی آن به سایر آسیب‌پذیری-ها در شبکه انجام می‌دهند بنابراین ارزیابی صحیحی از میزان خطر آسیب‌پذیری نخواهند داشت.

ارزیابی خطر یک آسیب پذیری به صورت منفرد یا بدون در نظر گرفتن ارتباط آن با سایر آسیب‌پذیری‌های موجود در یک شبکه، صحت ارزیابی خطر انجام شده را مختل می سازد و مانع از این می‌شود که اولویت‌بندی صحیحی از آسیب‌پذیری‌ها برای پیدا کردن پرخطرترین حملات داشته باشیم.

چالش بزرگی که در ارزیابی صحیح حملات از نقطه نظر برآورد خطر حملات چندمرحله‌ای وجود دارد این است که، در حال حاضر هیچ مرجعی برای یافتن ارتباط بین سیل عظیم آسیب‌پذیری‌های موجود در سیستم‌های کامپیوتری وجود ندارد. در نتیجه، بدون در اختیار داشتن مدل امنیتی گراف حمله یک سیستم کامپیوتری و تحلیل این مدل امنیتی ارزیابی خطر حملات چند مرحله‌ای در سیستم های کامپیوتری امری غیر ممکن است.

در [۲] ، تلاش شد، چالش سیستم‌های الگوی حمله موجود استخراج گردد و زیر بنایی برای توسعه مدل امنیتی حمله در آینده پیش‌بینی شد.

در این مقاله با هدف بهبود مقاله [۲]، یک سیستم مبتنی بر مدل امنیتی معرفی شد. بهبود مقاله حاضر نسبت به [۲]، عبارتست از :

- مدلی برای برآورد احتمال پویای رخداد حملات چند مرحله‌ای
- ارائه یک مدل امنیتی برای پیدا کردن زنجیره آسیب پذیری‌ها
- مدلی برای برآورد تاثیر مخرب رخداد حملات چند مرحله‌ای روی پارامترهای امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری

همچنین در [۳]، ما روشی برای ارزیابی خطر پویای حملات تک مرحله ای ارائه دادیم. در این مقاله ارزیابی خطر حملات تک مرحله‌ای با استفاده از معیارهای امنیتی موجود در این مقاله انجام شده است.

در ادامه بعد از مروری بر تعدادی از سیستم‌های ارزیابی خطر آسیب پذیری موجود، چالش‌های سیستم های موجود برای تعیین الگوی حمله بررسی می‌شود و سپس مدل پیشنهادی معرفی می‌گردد.

۲- مروری بر تعدادی از سیستم‌های ارزیابی خطر موجود

سیستم‌های امتیازدهی به دو صورت کیفی و کمی موجود هستند. در سیستم‌های کمی، براساس ویژگی‌های ذاتی و زمانی یک آسیب‌پذیری، یک عدد برای انعکاس سطح خطر آسیب‌پذیری مشخص می‌شود. در مقابل سیستم‌های کیفی قرار دارند که، شدت هر آسیب‌پذیری را در یکی از سطوح (پایین، متوسط، بالا و....) مشخص می سازند. روش های کمی گستره بالاتری از امتیازات را برای توصیف آسیب‌پذیری‌ها بکار می‌گیرند.

- مرکز پاسخ امنیتی مایکروسافت

این مرکز با هدف امن‌سازی عملکرد سیستم‌های مایکروسافت توسعه پیدا کرده است. ارائه گزارشاتی از آسیب‌پذیری‌های موجود در محصولات مایکروسافت نمونه‌ای از وظایف این مرکز است. سیستم سنجش شدت آسیب‌پذیری در مایکروسافت، پیامد بهره‌برداری از این آسیب‌پذیری را روی یک سیستم مشخص می‌سازد. پارامتر شدت آسیب‌پذیری، اطلاعاتی را در رابطه با احتمال بهره‌برداری از آسیب‌پذیری منعکس نمی‌سازد. بلکه، با این فرض که حمله صورت می‌گیرد، این سیستم امتیازدهی، بر اساس شدت حمله صورت گرفته روی سیستم از طریق بهره‌برداری از یک آسیب‌پذیری بخصوص، توصیه‌هایی را در رابطه با اعمال بروزرسانی‌ها برای محصولات خود منتشر می‌سازد. همچنین مایکروسافت، با هدف ارزیابی احتمال بهره‌برداری از آسیب پذیری‌ها به‌منظور بهینه‌سازی تصمیم‌گیری‌های امنیتی، اطلاعاتی را در رابطه با وضعیت ابزارهای بهره‌برداری از هر آسیب‌پذیری مشخص می‌سازد. محدود بودن ارزیابی خطر به آسیب‌پذیری‌های موجود در محصولات مایکروسافت و محدود بودن سطوح خطر از جمله نقاط‌ضعف سیستم امتیازدهی مایکروسافت محسوب می‌شوند.[۴]

- سیستم امتیازدهی Symantec

این سیستم امتیازدهی میزان خطر آسیب‌پذیری را در ۵ سطح کیفی مشخص می‌سازد. همچنین برای هر آسیب‌پذیری در کنار میزان خطر، راهکارهایی برای کاهش آثار منفی خطر نیز پیشنهاد شده است[۵].

- سیستم‌امتیازدهی RedHat

این سیستم امتیازدهی با الهام از پارامترهای سیستم امتیازدهی CVSS، میزان خطر آسیب‌پذیری‌های موجودر در محصولات شرکت Redhatرا مشخص می‌سازد. میزان خطر گزارش شده در این سیستم برای یک آسیب‌پذیری مشخص با مقدار اعلام شده توسط CVSS عموماً متفاوت است. چرا که، Redhatامتیازدهی به آسیب‌پذیری موجود در یک برنامه کاربردی را با درنظر گرفتن جایگاه آن در سکوی

مورد استفاده انجام می‌دهد. به بیان دیگر، میزان خطر بهره‌برداری از آسیب‌پذیری را با توجه به آسیبی که به کل سیستم وارد می‌کند، مشخص می‌سازد [۶].

- سیستم امتیازدهی به آسیب‌پذیری CVSS

این سیستم منعکس کننده تعدادی از خصوصیات ذاتی آسیب پذیری ها از جمله پیچیدگی بهره‌برداری از آسیب‌پذیری، سطح دسترسی مورد نیاز مهاجم روی شبکه برای بهره‌برداری از آسیب‌پذیری و تاثیر بهره‌برداری از تک آسیب‌پذیری‌های موجود روی سه پارامتر امنیتی محرمانگی، یکپارچگی و دسترسی‌پذیری است. CVSS با در نظر گرفتن پارامترهای مذکور، خطر متناظر با یک آسیب‌پذیری را به‌صورت کمی و کیفی مشخص می‌سازد. برای هر آسیب‌پذیری خطر یک آسیب‌پذیری با در اختیار داشتن مشخصه CVE قابل استخراج است[۷].

تعدادی سیستم امتیازدهی نیز با هدف بهبود سیستم‌های مذکور ارائه شده است که در ادامه به تعدادی از آنها اشاره شده است.

در [۸]، یک چارچوب مبتنی بر CVSS برای ارزیابی خطر در محیط‌های صنعتی از جمله IOT معرفی شده است.در [۹]، روشی برای پیدا کردن پر خطرترین آسیب‌پذیری های امنیتی با هدف بهبود دقت سیستم‌های امتیازدهی موجود ارائه شده است.در [۱۰]، روشی برای ارزیابی خطر حملات در حسگرها در محیط‌های هوشمند ارائه شده است.در [۱۱]، روشی برای ارزیابی شدت آسیب‌پذیری‌ها در اسکنر وب متن باز ارائه شده است.در [۱۲]، روشی برای زمانبندی اعمال اصلاحیه برای آسیب‌پذیری با اگاهی از میزان خطر پویای آسیب‌پذیری‌ها ارائه شده است.

در [۱۳]، یک روش امضای دیجیتالی مبتنی بر اصلاحیه ارائه شده است که امن‌سازی پیام را با پنهان‌سازی آن در یک تصویر انجام می‌دهد.در [۱۴] نیز، روشی برای تشخیص حمله فیشینگ در سیستم بانکی ارائه شده است

۳- معرفی مدل پیشنهادی

ارزیابی خطر یک آسیب پذیری نیازمند تخمین احتمال بهره برداری از یک آسیب‌پذیری و تاثیر بهره‌برداری شدن آن روی سه پارامتر امنیتی است.

چالش بزرگی که در ارزیابی صحیح حملات از نقطه نظر برآورد خطر حملات چندمرحله‌ای وجود دارد این است که، در حال حاضر هیچ مرجعی برای یافتن ارتباط بین سیل عظیم آسیب‌پذیری‌های موجود در سیستم‌های کامپیوتری وجود ندارد. در نتیجه، بدون در اختیار داشتن مدل امنیتی گراف حمله یک سیستم کامپیوتری و تحلیل این مدل امنیتی ارزیابی خطر حملات چند مرحله‌ای در سیستم های کامپیوتری امری غیر ممکن است.

در حال حاضر دو پایگاه داده از اطلاعات متناظر با آسیب‌پذیری‌ها موجود هستند که در ابتدای مرحله پیشنهاد پروژه این طرح پژوهشی به نظر می رسید در امر ارزیابی خطر حملات چند مرحله ای مفید باشند. این پایگاه‌های اطلاعاتی به شرح زیر هستند:

۱. CAPEC

در این پایگاه اطلاعاتی، حملات مختلف دسته‌بندی شده‌اند. همچنین این سیستم اطلاعاتی، پیش شرط‌های مورد نیاز برای بهره برداری از آسیب‌پذیری‌های موجود در هر حوزه را به همراه پیشنهاداتی برای اصلاح هر آسیب‌پذیری مشخص می‌سازد. تعدادی از حوزه های پوشش داده شده توسط CAPEC عبارتند از :

- مهندسی اجتماعی
- زنجیره تولید (تغییر به هنگام تولید و دستکاری به هنگام توزیع)
- ارتباطات (استراق سمع، دستکاری پروتکل و غیره)
- حملات نرم‌افزاری
- امنیت فیزیکی
- حملات سخت‌افزاری

معادل با هر الگوی حمله یک شناسه وجود دارد . همچنین امکان جستجو در CAPEC هم توسط این شناسه و هم براساس محتوا قابل انجام است[۱۵]

۲. CWE

در این پایگاه داده که به صورت مجانی برای استفاده عموم طراحی شده است، یک مجموعه یکپارچه از نقاط ضعف امنیتی را به همراه روش‌ها و ابزارهای موجود برای تشخیص و برطرف‌سازی این نقاط ضعف را به همراه تعدادی از آثار مخرب آنها مشخص می‌سازد[۱۶].

CWE را می‌توان یک لیست قراردادی از نقاط ضعف امنیتی دانست که:

- زبان مشترکی است برای توصیف نقاط ضعف امنیتی نرم افزا در معماری، طراحی و پیاده‌سازی.
- یک استاندادر عمومی است برای تشخیص ، سبک‌سازی و پیشگیری از حملات

در رابطه با سیسم اطلاعاتی CWE قابل توجه است که:

- معادل با هر نقطه ضعف یک شناسه وجود دارد که بر مبنای آن می‌توان اطلاعات مذکور در رابطه با نقطه ضعف امنیتی را استخراج کرد.
- بیش از ۱۰۰۰ نقطه ضعف ایندکس شده در سیستم CWE موجود است .

معادل با هر نقطه ضعف امنیتی در CWE، آسیب‌پذیری‌های متناظر با نقطه ضعف مرتبط وجود دارد.

با توجه به ماهیت CAPEC به نظر می‌رسد از آنجایی که این سیستم اطلاعاتی، توضیحاتی را در رابطه با رخداد هر الگوی حمله مشخص می‌کند بتواند منبع مفیدی برای استخراج زنجیره حملات باشد. اما، با توجه به چالش‌های یاد شده در بالا، از آنجایی که CAPEC اطلاعاتی

را در رابطه با هیچ نوع آسیب‌پذیری‌ای در اختیار قرار نمی‌دهد، نمی‌تواند به‌منظور استخراج الگوی حملات استفاده شود.

اما در رابطه با CWE صرفنظر از عدم سازگاری شناسه‌های متناظر با سه پایگاه داده مذکور برای استخراج اطلاعات، از آنجایی که این سیستم اطلاعاتی آسیب‌پذیری‌های متناظر با هر نقطه ضعف نرم افزاری را مشخص می‌سازد، می‌تواند به عنوان مرجعی برای پیدا کردن زنجیره آسیب‌پذیری‌ها مفید واقع شود.

در این مقاله، روشی ارائه شده است که با استناد به سیستم اطلاعاتی CWE بتواند ارزیابی‌ای از تعدادی از حملات چند مرحله‌ای داشته باشد. در ادامه ایده پیشنهادی معرفی شده است.

همان‌طور که اشاره شد، بیش از ۱۰۰۰ نوع نقطه ضعف نرم افزاری در CWE پیشنهاد شده است. آنالیز غیر خودکار این تعداد قابل توجه نقطه ضعف امنیتی (به دلیل فقدان اطلاعات مورد نیاز برای استخراج الگوی حملات) به منظور تعیین زنجیره حملات امری غیر کارا به شمار می آید. لذا در طرح پیش رو تلاش شده است براساس مستندات موجود، تعدادی از پرخطرترین و پررخدادترین نقاط ضعف امنیتی انتخاب و زنجیره حملات بر اساس این مجموعه امنیتی استخراج شود.

بعد از بررسی‌ها و مطالعات انجام شده در طرح حاضر مشخص شد که CWE تحت عنوان خطرناکترین ۲۵ خطای امنیتی معرفی شده توسط CWE/SANS مجموعه ای مهمترین نقاط ضعف امنیتی را مشخص می سازد [۱۶].

۲۵ نقطه ضعف نرم‌افزاری مذکور، فهرستی از شایع‌ترین و در عین حال خطرناک‌ترین خطاهای نرم افزاری هستند که می‌توانند منجر به حملات جدی در نرم افزارها شوند. این نقطه ضعف‌ها به‌سادگی توسط مهاجمان یافت می‌شوند و مورد بهره برداری قرار می‌گیرند. این نقطه ضعف‌ها بسیار خطرناک هستند. چرا که، به مهاجم این امکان را می‌دهند که به صورت مکرر به سیستم دسترسی پیدا کنند، داده سرقت کنند و مانع از این شوند که، سیستم به درستی کار کند.

CWE این ۲۵ نقطه ضعف خطرناک را به عنوان زیر مجموعه ای محدود اما مهم و فراگیر برای ارزیابی‌های امنیتی معرفی کرده است [۱۶]. رتبه‌بندی این ۲۵ نقطه ضعف امنیتی بر اساس سیستم CWSS* انجام شده است. نتایج این رتبه‌بندی در جدول (۱) نشان داده شده است. جزئیات پارامترهای دخیل در رتبه‌بندی نقاط ضعف امنیتی توسط CWSS در ادامه توضیح داده شده است.

پارامترهای دخیل در رتبه‌بندی نقاط ضعف امنیتی توسط CWSS به شرح زیر هستند:

۱. درجه شیوع نقطه ضعف امنیتی

ارزیابی این پارامتر توسط ۴ سطح کیفی موجود در جدول (۲) و براساس نظر متخصصان امنیتی انجام می‌شود:

۲. اهمیت نرم افزار

ارزیابی این فاکتور نیز با استفاده از ۴ سطح کیفی طبق جدول (۳) انجام می شود.

۳. پیامدهای مورد سوء استفاده قرار گرفتن نقطه ضعف

پیامدهی مورد سوء استفاده قرار گرفتن یک نقطه ضعف امنیتی در یکی از ۴ حوزه مشخص شده در جدول (۴) قرار می‌گیرد.

۴. احتمال بهره‌برداری از نقطه ضعف

این پارامتر با فرکانس رخداد حمله در حالتی که یک مهاجم مشخص و باتجربه وجود دارد، سنجیده می شود. ۳ سطح کیفی برای تخمین فرکانس رخداد حمله وجود دارد. این سطوح کیفی در جدول (۵) نشان داده شده است

۵. سادگی تشخیص

این پارامتر سهولت تشخیص نقطه ضعف توسط یک مهاجم حرفه‌ای را مشخص می‌کند. سهولت تشخیص یک نقطه ضعف نرم افزاری توسط مهاجم در سه سطح کیفی طبق جدول (۶) مشخص می‌شود.

۶. هزینه برطرف سازی یا کاهش اثرات مخرب نقطه ضعف

تفسیری از هزینه برطرف‌سازی توسط سه سطح کیفی در جدول جدول (۷) نشان داده شده است.

شش پارامتر فوق، فاکترهای اساسی بودند که برای تعیین خطرناک‌ترین نقاط ضعف مورد استفاده واقع می‌شوند. این فاکتورها به همراه زیر پارامترهای دیگری که در مستندات CWSS به آن اشاره شده است، طبق سیاست این سیستم امتیازدهی برای رتبه بندی نقطه ضعف‌ها مورد استفاده قرار می‌گیرد[۱۶].

با توجه به جامعیت ادعا شده توسط CWE در پوشش دهی حملات مرسوم توسط ۲۵ نقطه ضعف امنیتی مذکور، تلاش می شود استخراج الگوی حملات چند مرحله ای بر اساس این ۲۵ نقطه ضعف امنیتی انجام شود.

جدول (۱): خطرناکترین ۲۵ خطای امنیتی معرفی شده توسط CWE/SANS

ساده	این نقطه ضعف تقریباً هر روز توسط مهاجمان مورد سوء استفاده قرار می‌گیرد.
متوسط	تعدادی ابزار غیر خودکار برای تشخیص نقطه ضعفی از این نوع موجود هستند که وابسته به دانش مهاجم بوده و تحت شرایط خاصی این ابزارها قادر به تشخیص حمله خواهند بود.
دشوار	تشخیص نقطه ضعف توسط تعدادی ابزار دستی ممکن خواهد بود و این امر بسیار زمان‌بر و نیازمند تخصص مهاجم است.

جدول (۲): سطوح کیفی متناظر با پارامتر درجه شیوع

Rank	Score	ID	Name
[1]	93.8	CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
[2]	83.3	CWE-78	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
[3]	79.0	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')
[4]	77.7	CWE-79	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
[5]	76.9	CWE-306	Missing Authentication for Critical Function
[6]	76.8	CWE-862	Missing Authorization
[7]	75.0	CWE-798	Use of Hard-coded Credentials
[8]	75.0	CWE-311	Missing Encryption of Sensitive Data
[9]	74.0	CWE-434	Unrestricted Upload of File with Dangerous Type
[10]	73.8	CWE-807	Reliance on Untrusted Inputs in a Security Decision
[11]	73.1	CWE-250	Execution with Unnecessary Privileges
[12]	70.1	CWE-352	Cross-Site Request Forgery (CSRF)
[13]	69.3	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
[14]	68.5	CWE-494	Download of Code Without Integrity Check
[15]	67.8	CWE-863	Incorrect Authorization
[16]	66.0	CWE-829	Inclusion of Functionality from Untrusted Control Sphere
[17]	65.5	CWE-732	Incorrect Permission Assignment for Critical Resource
[18]	64.6	CWE-676	Use of Potentially Dangerous Function
[19]	64.1	CWE-327	Use of a Broken or Risky Cryptographic Algorithm
[20]	62.4	CWE-131	Incorrect Calculation of Buffer Size
[21]	61.5	CWE-307	Improper Restriction of Excessive Authentication Attempts
[22]	61.1	CWE-601	URL Redirection to Untrusted Site ('Open Redirect')
[23]	61.0	CWE-134	Uncontrolled Format String
[24]	60.3	CWE-190	Integer Overflow or Wraparound
[25]	59.9	CWE-759	Use of a One-Way Hash without a Salt

جدول (۳): سطوح کیفی متناظر با پارامتر اهمیت نرم افزار

ضروری	این نقطه ضعف باید هر چه سریعتر برطرف شود.
بالا	این نقطه ضعف نیز باید سریعاً برطرف شود. اما خطر آن از سطح "ضروری" کمتر است.
معمولی	به این نقطه ضعف بعد از دو سطح " ضروری" و "بالا" رسیدگی می شود.
محدود	رسیدگی به این نقطه ضعف ضروری نیست.

جدول (۴): سطوح مختلف از پیامدهای سوء استفاده از نقطه ضعف

اجرای کد	مهاجم قادر است کد یا دستوراتی را اجرا کند.
فقدان داده	مهاجم می‌تواند داده های حساس را سرقت کند، آنها را تغییر دهد یا خراب کند.
عدم پذیرش سرویس	به این نقطه ضعف بعد از دو سطح " ضروری" و "بالا" رسیدگی می شود..

جدول (۵): سطوح کیفی متناظر با پارامتر احتمال بهره برداری از نقطه ضعف

اغلب	این نقطه ضعف تقریباً هر روز توسط مهاجمان مورد سوء استفاده قرار می‌گیرد.
گاهی اوقات	این نقطه ضعف تقریباً ماهی یکبار اتفاق می افتد.
به ندرت	این نقطه ضعف کمتر از یکبار در ماه اتفاق می افتد.

جدول (۶): سطوح کیفی متناظر با پارامتر سادگی تشخیص

شایع	این نقطه ضعف نسبت به سایر نقطه ضعف‌ها با درصد بالاتری منجر به حمله می‌شود
بالا	این نقطه ضعف اغلب ولی نه به صورت گسترده توسط مهاجمان مورد بهره‌برداری قرار می‌گیرد.
معمولی	نقطه ضعف به صورت دوره‌ای منجر به حمله می‌شود.
محدود	نقطه ضعف متناسب با این سطح کیفی به ندرت مورد حمله مهاجمان قرار می‌گیرد یا هرگز منجر به حمله نمی شود

جدول (۷): سطوح کیفی متناظر با پارامتر هزینه برطرف سازی

پایین	برطرف‌سازی نقطه ضعف امنیتی نیازمند تغییر در یک بلاک یا تابع است.
متوسط	برای برطرف‌سازی آسیب پذیری نیازمند تغییر در کد یا الگوریتم یافایل یا یک جزء از نرم افزار هستیم
بالا	برطرف سازی نقطه ضعف نیازمند تغییرات اساسی در طراحی یا معماری است.

ایده اصلی روش ارائه شده در تعیین زنجیره آسیب‌پذیری از این واقعیت ناشی می‌شود که، چون هر آسیب پذیری ناشی از یک نقطه ضعف نرم افزاری است، مسئله پیدا کردن ارتباط بین آسیب‌پذیری‌ها از نقطه نظر چگونگی بهره برداری از آسیب پذیری‌ها در رخداد حملات چند مرحله‌ای را می توان معادل با مسئله پیدا کردن ارتباط بین نقاط ضعف امنیتی متناظر با آسیب‌پذیری‌ها دانست. بنابراین در این مرحله تلاش می‌شود روشی برای پیدا کردن چگونگی ارتباط بین این نقاط ضعف امنیتی پیشنهاد شود.

ایده تخمین خطر حملات چند مرحله ای توسط سیستم CWE، با مطالعه عملکرد این سیستم اطلاعاتی و بررسی داده های قابل استخراج توسط هر شناسه CWE انجام شده است. در ادامه، خلاصه ای از فیلدهای قابل استخراج توسط شناسه های CWE ارائه شده است.

سیستم CWE متناظر با هر شناسه، اطلاعاتی به شرح زیر را مشخص می سازد:

- توصیفی از نقطه ضعف امنیتی
- مرحله‌ای از توسعه نرم افزار که نقطه ضعف ایجاد شده است
- میزان آسیب بهره‌برداری از نقطه ضعف توسط مهاجم به پارامترهای امنیتی
- روش‌های تشخیص نقطه ضعف توسط مهاجم
- آسیب‌پذیری‌های متناظر با نقطه ضعف فوق در قالب شناسه CVE
- روش‌های موجود برای تخفیف و سبک‌سازی نقطه ضعف امنیتی
- منابع سیستمی که در نتیجه بهره‌برداری نقطه ضعف آسیب می‌بینند
- الگوهای حمله متناظر با این نقطه ضعف امنیتی در قالب شناسه CAPEC
- چگونگی ارتباط این نقطه ضعف با سایر نقطه ضعف‌های امنیتی

تعدادی از ارتباطات ممکن بین یک نقطه ضعف امنیتی و سایر نقاط ضعف امنیتی به شرح زیر:

- Child

این نقطه ضعف امنیتی ، زیر مجموعه ای از دامنه بزرگتری است. در این حالت، ارتباط معکوس بین این نقطه ضعف متناظر و نقطه ضعف مذکور، Parent خواهد بود.

- Parent
- Requires

وجود این ارتباط بدین معناست که، برای مورد سوء استفاده واقع شدن این نقطه ضعف امنیتی توسط مهاجم، بهره برداری از نقاط ضعف دیگری الزامی است که توسط این فیلد مشخص می‌شود. در این حالت، ارتباط معکوس بین این نقطه ضعف و نقطه ضعف مذکور از نوع Required by خواهد بود.

- Required by
- Can follow
- منظور از این نوع ارتباط آن است که، بهره برداری از این نقطه ضعف می‌تواند بعد از مورد سوء استفاده شدن نقطه ضعفی انجام شود که توسط این فیلد مشخص می شود. در این حالت ارتباط معکوس بین این نقطه ضعف و نقطه ضعف مذکور از نوع Can precede خواهد بود
- Can precede

در بین فیلدهای مذکور از اطلاعات قابل استخراج توسط CWE، تنها مورد آخر (چگونگی ارتباط این نقطه ضعف با سایر نقطه ضعف های امنیتی) می تواند برای پیدا کردن چگونگی ارتباط بین نقاط ضعف امنیتی مفید باشد. در مورد آخر، انواع ممکن از چگونگی ارتباط بین یک نقطه ضعف امنیتی و سایر نقاط ضعف امنیتی به ایجاز بیان شد و در ادامه تلاش شده است این الگوی ارتباطاتی برای ۲۵ نقطه ضعف خطرناک معرفی شده توسط CWE، استخراج شود.

باید دقت داشت که، در فیلد "چگونگی ارتباط این نقطه ضعف با سایر نقطه ضعف‌های امنیتی" ارتباطات از نوع Requires، Required by، Can Precede و Can Follow می‌توانند چگونگی ارتباط بین نقاط ضعف نرم افزاری را مشخص کنند .

مراحل استخراج ارتباط بین نقطه ضعف‌های نرم افزاری به شرح زیر است:

۱. برای هر یک از ۲۵ نقطه ضعف نرم افزاری مذکور که در زمره خطرناک‌ترین نقطه ضعف‌ها معرفی شده اند، ارتباطات از نوع Requires، Required by، Can Precede و Can Follow استخراج شده‌اند و نتایج در جدول (۸) نشان داده شده است.

ارتباطات مذکور بین هر نقطه ضعف و سایر نقاط ضعف موجود می‌تواند انعکاسی از ترتیب بهره برداری شدن از نقاط ضعف موجود در یک سیستم برای وقوع حمله باشد.

هدف اصلی در این پژوهش، انجام ارزیابی خطر یک آسیب‌پذیری با در نظر گرفتن ارتباط آن با سایر آسیب‌پذیری‌ها است. لذا باید بتوان با استفاده از ارتباطات استخراج شده در این مرحله، ارزیابی خطر یک آسیب‌پذیری را با توجه به رابطه نقطه ضعف متناظر با آن آسیب‌پذیری و سایر نقاط ضعف موجود در سیستم انجام داد.

طبق تعریف، میزان خطر یا ریسک به‌صورت (۱) محاسبه می‌شود:

$$Risk=Probability\times Impact \quad (۱)$$

پارامترهای موجود در (۱) به شرح زیر هستند:

- Risk : میزان خطر بهره برداری شدن یک آسیب‌پذیری روی یک سیستم است.
- Impact : تاثیر بهره برداری از آسیب پذیری روی پارامترهای امنیتی محرمانگی، یکپارچگی و دسترسی پذیری
- Probability : احتمال رخداد حمله

تخمین صحیح احتمال مورد بهره‌برداری واقع شدن یک آسیب‌پذیری با برآورد دو مورد زیر ممکن خواهد بود:

- احتمال ذاتی رخداد یک آسیب پذیری

زیر معیار Exploitability از نسخه ۳ سیستم CVSS را می‌توان معیار مناسبی برای ارزیابی خصوصیات ذاتی یک آسیب‌پذیری دانست. لذا در طرح پیش رو معیاری امنیتی برای ارزیابی احتمال ذاتی رخداد یک آسیب پذیری (رابطه (۲)) تعریف شده است.

$$\text{Prob(Intrinsinc)} = \frac{\text{Exploitability}}{10} \qquad (۲)$$

- احتمال پویای بهره‌برداری از یک آسیب‌پذیری

در [۳] روشی مبتنی بر توزیع‌های احتمال برای ارزیابی احتمال پویای بهره‌برداری از یک آسیب‌پذیری پیشنهاد شد. روش مذکور با ارزیابی دو فاکتور زیر ابزاری را برای تخمین احتمال پویای بهره برداری از آسیب پذیری ها در اختیار قرار می‌دهد:

- احتمال وجود اصلاحیه برای یک آسیب‌پذیری در یک نقطه مشخص از زمان
- احتمال وجود اکسپلویت برای بهره‌برداری از یک آسیب‌پذیری در یک زمان بخصوص

احتمال‌های مذکور طبق توضیحات موجود در [۳] با استفاده از دو توزیع احتمال Pareto و Weibull محاسبه می‌شوند و با در نظر گرفتن سن آسیب‌پذیری تخمین زده می‌شوند.

این روش، پوشش کاملی از فاکتوهای زمانی در تخمین احتمال بهره‌برداری از آسیب‌پذیری ندارند و باید تلاش شود که روش دیگری برای تخمین احتمال پویای بهره‌برداری از آسیب‌پذیری‌ها پیشنهاد شود که محدوده وسیع‌تری از عوامل زمانی را پوشش دهد.

در این رابطه باید دقت داشت که، در محاسبه رتبه[1] نقاط ضعف امنیتی (جدول (۱)) که توسط CWSS انجام شده است، فاکتورهای زمانی متعددی از جمله موارد زیر در تعیین رتبه مذکور تاثیر گذار بوده‌اند:

- درجه شیوع نقطه ضعف امنیتی در نرم افزارها
- سادگی تشخیص (کیفیت امکانات مورد نیاز برای تشخیص نقطه ضعف)
- فرکانس رخداد حمله با توجه به دانش و مهارت مهاجمان
- سادگی بهره‌برداری (احتمال موجود بودن اکسپلویت برای سوء استفاده از نقطه ضعف)
- کیفیت اصلاحیه‌ها و ابزارهای مورد نیاز برای مقابله با نقطه ضعف

از آنجایی که پوشش‌دهی CWSS از نقطه نظر عوامل زمانی نسبت به روش پیشنهادی در [۹] بالاتر است به منظور ارزیابی احتمال پویای بهره‌برداری از یک آسیب‌پذیری، در این مقاله، روشی مبتنی بر ویژگی‌های نقطه ضعف‌های امنیتی متناظر با هر آسیب‌پذیری برای ارزیابی احتمال پویای بهره‌برداری از آسیب‌پذیری‌ها پیشنهاد شده است. ویژگی‌های روش ارائه شده به شرح زیر هستند:

- احتمال پویای یک نقطه ضعف با استفاده از نتیجه مرحله ۲ از فرآیند استخراج ارتباط بین نقطه ضعف های نرم افزاری (چگونگی ارتباط آن با سایر نقاط ضعف موجود در سیستم) تخمین زده می‌شود.
- احتمال پویای بهره برداری از یک آسیب پذیری برابر خواهد بود با احتمال پویای نقطه ضعف متناظر با آن.

در نتیجه، فرآیند ارزیابی خطر حملات چند مرحله‌ای به مسئله پیدا کردن احتمال پویای بهره‌برداری از یک آسیب‌پذیری تبدیل شده است. در ادامه (مرحله دوم از فرآیند استخراج ارتباط بین نقطه ضعف های نرم افزاری) روش پیشنهادی معرفی می‌شود.

۲. استخراج احتمال مورد بهره‌برداری واقع شدن یک نقطه ضعف به منظور ارزیابی خطر حملات چند مرحله‌ای

در روش پیشنهادی مسئله ارزیابی خطر حملات چند مرحله‌ای با مسئله تخمین احتمال پویای رخداد یک نقطه ضعف امنیتی با در نظر گرفتن چگونگی ارتباط آن با سایر نقاط ضعف امنیتی موجود در یک سیستم، معادل دانسته شده است. لذا در این پژوهش تلاش شده است تا، روشی برای ارزیابی احتمال پویای یک نقطه ضعف با در نظر گرفتن ارتباط آن با سایر نقاط ضعف موجود دریک سیستم ارائه شود.

احتمال مذکور طی مراحل زیر محاسبه می‌شود:

الف) ارزیابی احتمال پویای مورد بهره‌برداری واقع شدن یک نقطه ضعف نرم افزاری واحد

همان‌طور که پیش از این نیز اشاره شد، هر آسیب‌پذیری در نتیجه سوء استفاده از نقطه ضعف نرم افزاری متناظر با آن مورد بهره‌برداری قرار می‌گیرد. لذا، از آنجایی که انعکاس عوامل زمانی در قالب امتیاز CWSS برای ۲۵ نقطه ضعف نرم افزاری پرخطر در دسترس است و این نقطه ضعف‌ها طبق ادعای CWE پوشش دهنده سیل وسیعی از آسیب‌پذیری‌های موجود هستند، در طرح حاضر تلاش شده است که، روشی برای تخمین احتمال پویای بهره‌برداری شدن ۲۵ نقطه ضعف خطرناک ارائه شود.

با توجه به پوشش جامع CWSS از عوامل زمانی در رتبه‌بندی نقطه ضعف‌های نرم افزاری، معیاری امنیتی برای تخمین احتمال پویای مورد بهره‌برداری واقع شدن یک نقطه ضعف امنیتی پیشنهاد شده است. (رابطه (۳))

$$\text{Prob(Intrinsinc)} = \frac{CWSS}{100} \qquad (۳)$$

(دقت شود که امتیاز اعلام شده برای هر نقطه ضعف امنیتی، توسط محاسبه گر CWSS در محدوده ۰ تا ۱۰۰ قرار دارد.)

به عنوان یک جمع‌بندی از این بخش می‌توان گفت، احتمال پویای مورد بهره‌برداری واقع شدن یک آسیب‌پذیری برابر خواهد بود با حاصل رابطه (۳) برای نقطه ضعف متناظر با آن.

ب) ارزیابی احتمال مورد بهره برداری واقع شدن زنجیره‌ای از نقطه ضعف‌ها

روش ارائه شده در طرح پیش رو برای ارزیابی خطر حملات براساس این واقعیت ارائه شده است که، حملات واقعی در شبکه‌های کامپیوتری حملات چند مرحله‌ای هستند که از بهره‌برداری از چندین آسیب پذیری با یک ترتیب مشخص به وقوع می‌پیوندند. بنابراین، ارزیابی خطر یک آسیب‌پذیری با در نظر گرفتن ارتباط آن با سایر آسیب‌پذیری‌ها، از ضروریات به نظر می رسد.

همان‌طور که پیش‌تر نیز بدان اشاره شد، ارزیابی خطر یک آسیب‌پذیری با در نظر گرفتن ارتباط آن با سایر آسیب‌پذیری‌ها را می‌توان با ارزیابی خطر نقطه ضعف متناظر با آسیب پذیری مورد نظر و سایر نقاط ضعف موجود در سیستم معادل دانست.

در طرح پیش رو ارتباطات از نوع Requires، Required by، Can Precede و Can Follow که پیش‌تر بدان اشاره شد، به عنوان ابزاری برای برآورد احتمال مورد سوء استفاده واقع شدن یک نقطه ضعف با در نظر گرفتن ارتباط آن با سایر نقاط ضعف موجود در سیستم استفاده می‌شود. بسته به نوع ارتباط یک نقطه ضعف با سایر نقاط ضعف موجود، روش ارزیابی خطر مورد بهره‌برداری واقع شدن یک نقطه ضعف به شرح زیر متفاوت خواهد بود:

- ارتباط از نوع Requires : زمانی که یک نقطه ضعف دارای ارتباطی از نوع Requires با سایر نقطه ضعف ها است، بدین معناست که مورد سوء استفاده واقع شدن یک نقطه ضعف نیازمند مورد بهره‌برداری شدن تمامی آن نقطه ضعف‌ها است. بنابراین می‌توان ادعا داشت که، احتمال مورد بهره‌برداری واقع شدن منفرد هر یک از نقاط ضعفی که دارای ارتباطی از نوع Requires با یک نقطه ضعف مخصوص هستند، با احتمال بهره برداری از آن برابر است. (رابطه (۴))

$$prob(Required\_CWE)= Prob(Main\_CWE) \quad (۴)$$

مثالی از این نمونه، ارتباط نقطه ضعف CWE-352 است. طبق اطلاعات موجود در جدول (۸)، بهره‌برداری از این نقطه ضعف، نیازمند آن است که نقطه ضعف‌های زیر در سیستم مورد بهره‌برداری واقع شوند.

- ✓ CWE-642
- ✓ CWE-613
- ✓ CWE-441
- ✓ CWE-346

- ارتباط از نوع Can Follow : ارتباط از نوع Can Follow یک نقطه ضعف با سایر نقطه ضعف‌ها، بدین معناست که نقطه ضعف مذکور می‌تواند در نتیجه مورد سوء استفاده واقع شدن هر یک از آنها در سیستم مورد بهره‌برداری قرار بگیرد. به عبارت دیگر این ارتباط، به تعدادی از عواملی که می‌توانند بهره‌برداری از نقطه ضعف مذکور را منجر شوند اشاره می‌کند.

تفاوت ارتباط از نوع Can Follow با Requires را می‌توان به صورت زیر تحلیل کرد:

در Requires ارتباط بین نقطه ضعف‌های مورد نیاز از نوع AND است. در صورتی که در Can Follow ، ارتباط بین نقطه ضعف‌های مورد نیاز از نوع OR است.

در ارتباطات از نوع Can Follow، عاملی به غیر از نقاط ضعف دارای ارتباط با نقطه ضعف مذکور نیز می‌توانند در بهره برداری از نقطه ضعف مذکور موثر باشند.

با توجه به توضیحات مذکور، احتمال بهره‌برداری منفرد از هر یک از نقاط ضعفی که با نقطه ضعف مورد نظر دارای ارتباط Can Follow هستند با استفاده از معیار پیشنهادی در رابطه (۵) محاسبه می‌شود.

$$Prob(preceder\_CWE)= \frac{Prob(Main\_CWE)}{Num\_of\_Preceders} \quad (۵)$$

دقت شود که هدف اصلی از بررسی ماهیت ارتباطات، ارزیابی احتمال پویای مورد بهره‌برداری واقع شدن یک نقطه ضعف با در نظر گرفتن چگونگی ارتباط آن با سایر نقاط ضعف موجود در سیستم است.

برآورد این احتمال پویا نیازمند تعریف تعدادی معیار امنیتی مبتنی بر نوع ارتباط به شرح زیر است:

- ✓ استخراج احتمال بهره برداری منفرد از نقاط ضعفی که با نقطه ضعف مربوطه دارای ارتباطلاتی از نوع Can Follow و Requires هستند.

چگونگی برآورد این احتمال برای ارتباط از نوع Requires در رابطه (۴) و برای ارتباطات از نوع Can Follow در رابطه (۵) توضیح داده شده است.

- ✓ چگونگی تلفیق احتمال پویای بهره‌برداری شدن زنجیره‌ای از نقطه ضعف‌ها با استفاده از احتمال بهره‌برداری منفرد از نقاط ضعفی که در ارتباط با نقطه ضعف مورد نظر هستند.

در ادامه معیارهای امنیتی پیشنهادی برای ارزیابی خطر زنجیره نقطه ضعف‌های امنیتی معرفی می‌شوند. این

معیارهای امنیتی که معیارهایی مبتنی بر ارتباط هستند برای هر یک از دو ارتباط Can Follow و Requires به شرح زیر هستند:

برآورد احتمال پویای بهره‌برداری از یک نقطه ضعف توسط مهاجم با در نظر گرفتن نقاط ضعفی که آسیب‌پذیری با آنها دارای ارتباط از نوع Requires است با استفاده از معیار امعیار امنی پیشنهادی در رابطه (۶) ممکن خواهد بود.

❖ ارتباط از نوع Requires :

برآورد احتمال پویای بهره‌برداری از یک نقطه ضعف توسط مهاجم با در نظر گرفتن نقاط ضعفی که آسیب‌پذیری با آنها دارای ارتباط از نوع Requires است با استفاده از معیار امنیتی پیشنهادی در رابطه (۶) ممکن خواهد بود.

$$Prob(Chain\_Main\_CWE)= Prob(Required\_CWE)\times Prob(Main\_CWE) \quad (۶)$$

❖ ارتباط از نوع Can Follow:

چگونگی تخمین احتمال پویای مورد سوء استفاده واقع شدن نقطه ضعفی که دارای ارتباط از نوع Can Follow با سایر نقطه ضعف‌ها است، با استفاده از معیار امنیتی رابطه (۷) قابل تخمین است.

$$Prob(Chain\_Main\_CWE)= Max(Prob(Preceder\_CWE))\times Prob(Main\_CWE) \quad (۷)$$

در رابطه (۷)، منظور از $Max(Prob(Preceder\_CWE))$، تمامی نقاط ضعفی هستند که دارای ارتباط از نوع Can Follow با نقطه ضعف مورد نظر باشند.

احتمال رخداد زنجیره نقطه ضعف‌ها را احتمال جمعی نیز می‌توان نامگذاری کرد.

نکته قابل توجه این است که، یک نقطه ضعف ممکن است برای بیش از یکی از ۲۵ نقطه ضعف خطرناک معرفی شده توسط CWE ، نقش precede (پیش‌رو) یا Required By را داشته باشد. در این حالت، احتمال منفرد برای هر یک از پیش‌روها یا نقطه ضعف‌هایی که دارای ارتباط از نوع Required By با آسیب‌پذیری مذکور هستند محاسبه می شود و ماکزیمم این مقادیر به عنوان احتمال منفرد یک نقطه ضعف با نقش پیش‌رو یا Required By معرفی می‌شود. CWE-456 نمونه‌ای از این حالت خاص است که در نقش Can Precede برای CWE-89 و CWE-120 قرار دارد.

احتمال جمعی سوء استفاده از یک نقطه ضعف و همچنین احتمال منفرد بهره برداری از نقاط ضعفی که در ارتباط با آن آسیب‌پذیری هستند توسط معیارهای امینتی پیشنهادی (روابط (۴) تا (۷)) محاسبه شده و نتایج در جدول (۹) و شکل (۱) قابل مشاهده است. نقاط ضعفی که در جدول و شکل ذکر نشده‌اند، نقاط ضعفی هستند که احتمال منفرد (محاسبه شده توسط رابطه (۳) و جمعی آنها برابر هستند.

۳-۱- استخراج احتمال پویای رخداد حملات چند مرحله‌ای با استفاده از احتمال پویای زنجیره نقطه ضعف‌ها

همان‌طور که در بخش‌های قبل به آن اشاره شد در این پژوهش بنا به دلایل ذکر شده، مسئله ارزیابی خطر بهره‌برداری از یک آسیب‌پذیری با در نظر گرفتن ارتباط آن با سایر آسیب‌پذیری‌ها به مسئله ارزیابی خطر احتمال مورد سوء استفاده قرار گرفتن یک نقطه ضعف با در نظر گرفتن چگونگی ارتباط آن با سایر نقطه ضعف‌ها تبدیل شده است.

تا به این مرحله، چگونگی استخراج احتمال حمله به یک نقطه ضعف امنیتی با در نظر گرفتن زنجیره نقطه ضعف متناظر با آن معرفی شد (منظور نقطه ضعف‌هایی است که با آن در ارتباط هستند). این احتمال مطابق مراحل زیر برای ارزیابی خطر جمعی یک آسیب‌پذیری مورد استفاده قرار می‌گیرد:

۱. استخراج نقطه ضعف متناظر با آسیب پذیری از پایگاه داده NVD
۲. تخمین احتمال مورد سوء استفاده قرار گرفتن نقطه ضعف حاصل از مرحله ۱ با استفاده از معیارهای امنیتی معرفی شده در این طرح پژوهشی (روابط (۳) تا (۷))
۳. محاسبه احتمال بهره برداری از آسیب پذیری (M.Exploitability) با استفاده از روش معرفی شده در [۹]. در این مقاله احتمال ذاتی و پویای آسیب پذیری تواما برای تخمین احتمال استفاده می شود. پارامتر Prob(Chain_Main_CWE) به عنوان معیار احتمال پویا در روش [۳] جایگزین می‌شود.
۴. محاسبه پارامتر Impact با استفاده از روش [۳].
۵. استفاده از نتایج مراحل ۳و۴ برای ارزیابی خطر آسیب پذیری با استفاده از رابطه (۱)

۳-۲- اعمال روش پیشنهادی برای ارزیابی خطر تعدادی آسیب‌پذیری منتخب

در این بخش، نتایج ارزیابی خطر تعدادی آسیب‌پذیری با استفاده از روش پیشنهادی بیان شده است.

از آنجایی که سیستم‌های امتیازدهی به آسیب‌پذیری موجود ارزیابی خطر را برای حملات تک مرحله‌ای انجام می‌دهند، مقایسه کمی سیستم پیشنهادی با سیستم‌های موجود ممکن نیست.

انتخاب آسیب‌پذیری‌های تحت تست با این هدف انجام شده است تا، بهبودهای سیستم پیشنهادی نسبت به CVSS در ارزیابی

خطر آسیب‌پذیری‌ها مشهود باشد. به عبارت دیگر تلاش شده است تا آسیب‌پذیری‌هایی برای تست انتخاب شوند که، در نتیجه بهره‌برداری از تعداد دیگری آسیب‌پذیری در سیستم، مورد سوء استفاده قرار می‌گیرند و مورد حمله واقع شدن آن‌ها به صورت منفرد ممکن نباشد. در نتیجه، تعدادی آسیب پذیری از مجموعه نقطه ضعف هایی انتخاب شده‌اند که، طبق جدول (۸) با سایر نقطه ضعف‌ها دارای ارتباطاتی از نوع Requires و Can Follow باشند. این تعداد آسیب‌پذیری به همراه نتایج ارزیابی خطر و پارامترهای مرتبط در جدول (۱۰) نشان داده شده‌اند. در جدول مذکور، پارامترهای ذکر شده توسط روش [۳] محاسبه شده است.

ارزیابی خطر آسیب پذیری‌های متناظر با ۲۵ نقطه ضعف امنیتی توسط CVSS بدون در نظر گرفتن الگوی حمله انجام می‌شود. لذا با تخمین خطر آسیب پذیری های مذکور توسط CVSS، ارزیابی خطر از وقوع حمله واقعی انجام نخواهد شد. اما، ارزیابی خطر انجام شده توسط سیستم پیشنهادی برای آسیب‌پذیری‌های مذکور با در نظر گرفتن الگوی حمله موجود متناظر با آسیب‌پذیری است

۴- نتیجه‌گیری

مدیریت کارای خطر به‌منظور بقای عملیات تجاری و انجام ماموریت‌های سازمانی امری ضروری به‌نظر می‌رسد. افزایش سیستم‌ها، شبکه‌ها، برنامه‌های کاربردی، ابزارهای سیار و تمایل به سمت و سوی مجازی‌سازی و محاسبت ابری، می‌تواند محیطی را ایجاد کند که، نرخ بروز حملات در آن سیر روزافزونی دارد. از اطلاعات محرمانه تجاری و اختصاصی گرفته تا گزارشات حساس پزشکی به دلیل جریان‌های داده مهمی که در این سیستم‌ها وجود دارد در معرض حملات قرار دارند.

در فرآیند تعیین خطر، در اختیار داشتن مدل امنیتی کارا به منظور تخمین کمی از خطر حملات چند مرحله‌ای یا زنجیره آسیب پذیری امری ضروری به نظر می‌رسد.

ایده اصلی در تعیین زنجیره آسیب‌پذیری از این واقعیت ناشی می شود که، از آنجایی که هر آسیب پذیری ناشی از یک نقطه ضعف نرم افزاری است، مسئله پیدا کردن ارتباط بین آسیب‌پذیری‌ها از نقطه نظر چگونگی بهره برداری از آسیب پذیری‌ها در رخداد حملات چند مرحله ای را می توان معادل با مسئله پیدا کردن ارتباط بین نقاط ضعف امینتی متناظر با آسیب‌پذیری‌ها دانست. در این پژوهش تلاش شد، بر اساس ۲۵ نقطه ضعف امنیتی مهم گزارش شده توسط CWE مدلی برای ارزیابی خطر حملات چند مرحله ای ارائه شود.

با وجود تلاش‌های انجام شده در جهت توسعه هر چه کامل‌تر و دقیق‌تر سیستم پیشنهادی، کمبودهایی نیز در طرح به انجام رسیده وجود دارد که کوشش می‌شود در پژوهش‌های آتی برطرف شود. از جمله مواردی که در سیستم پیشنهادی لحاظ نشده است، عدم توانایی در ارزیابی خطر حملات روز صفر است. حملات روز صفر حملاتی هستند که، برای مهاجمان شناخته شده هستند اما اطلاعاتی در رابطه با عوامل بروز این حملات در پایگاه‌داده‌هایی مانند NVD وجود ندارد به عبارت دیگر هیچ شناسه‌ای همانند حملات شناخته شده برای آنها وجود ندارد.

در روش پیشنهادی، ارزیابی خطر با استفاده از شناسه CVE یک آسیب‌پذیری انجام می‌شود. بنابراین در این سیستم امکان ارزیابی خطر حملات ناشناخته وجود ندارد. در نتیجه در کارهای آتی تلاش خواهد شد، سیستم پیشنهادی به شکلی بهبود یابد که، ارزیابی این گونه حملات نیز توسط آنها ممکن باشد.

جدول (۸): الگوی ارتباطی ۲۵ نقطه ضعف خطرناک با سایر نقطه ضعف‌ها

	Requires	Required by	Can Precede	Can Follow	Prob_Intrinsinc
CWE-89				CWE-456	۰.۹۳۸
CWE-78				CWE-184	۰.۸۳۳
CWE-120				CWE-456 CWE-416 CWE-242 CWE-231 CWE-170	۰.۷۹
CWE-79			CWE-494	CWE-113 CWE184	۰.۷۷۷
CWE-306					۰.۷۶۹
CWE-862					۰.۷۶۸
CWE-798					۰.۷۵

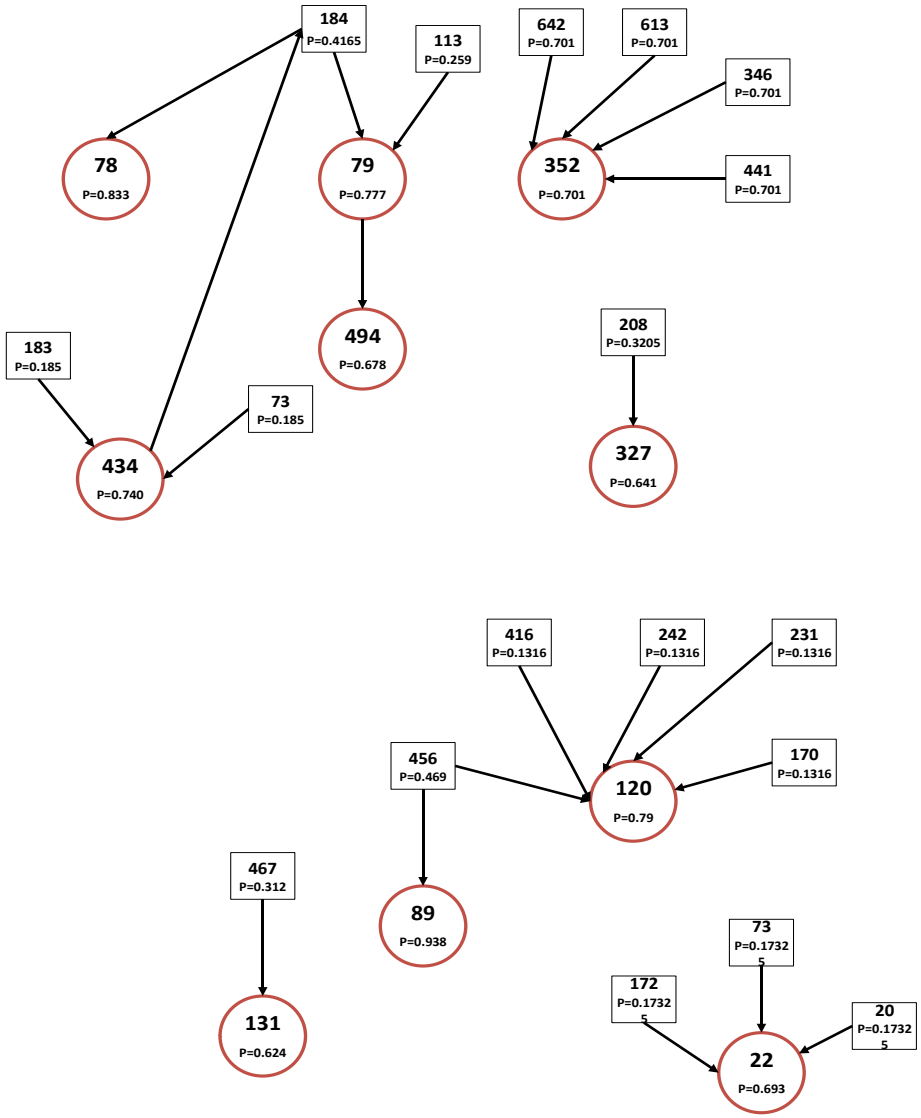
CWE-311					۰.۷۵
CWE-434				CWE-73 CWE-183 CWE-184	۰.۷۴
CWE-807					۰.۷۳۸
CWE-250					۰.۷۳۱
CWE-352	CWE-642 CWE-613 CWE-441 CWE346				۰.۷۰۱
CWE-22				CWE-172 CWE-73 CWE-20	۰.۶۹۳
CWE-494				CWE-79	۰.۶۸۵
CWE-863					۰.۶۸۷
CWE-829					۰.۶۶
CWE-732					۰.۶۵۵
CWE-676					۰.۶۴۶
CWE-327				CWE-208	۰.۶۴۱
CWE-131				CWE-467	۰.۶۲۴
CWE-601					۰/۶۱۱
CWE-134					۰/۶۱۰
CWE-190					۰/۶۰۳
CWE-759					۰/۵۹۹

جدول (۹): احتمال جمعی سوء استفاده از ۲۵ نقطه ضعف خطرناک

نقطه ضعف	Prob(Chain_Main_CWE)	نقطه ضعف	Prob(Chain_Main_CWE)
CWE-78	۰/۸۳۳	CWE-642	۰/۷۰۱
CWE-79	۰/۷۷۷	CWE-613	۰/۷۰۱
CWE-352	۰/۷۰۱	CWE-441	۰/۷۰۱
CWE-494	۰/۶۷۸	CWE-346	۰/۷۰۱
CWE-434	۰/۷۴	CWE-208	۰/۳۲۰۵
CWE-327	۰/۶۴۱	CWE-184	۰/۴۱۶۵
CWE-89	۰/۹۳۸	CWE-113	۰/۲۵۹
CWE-120	۰/۷۹	CWE-73	۰/۱۸۵
CWE-22	۰/۶۹۳	CWE-183	۰/۱۸۵
CWE-131	۰/۶۲۴	CWE-456	۰/۴۶۹
CWE-416	۰/۱۳۱۶	CWE-242	۰/۱۳۱۶
CWE-231	۰/۱۳۱۶	CWE-170	۰/۱۳۱۶
CWE-20	۰/۱۷۳۲۵	CWE-73	۰/۱۷۳۲۵
CWE-172	۰/۱۷۳۲۵	CWE-467	۰/۳۱۲

جدول (۱۰): نتایج اعمال روش پیشنهادی روی تعدادی آسیب پذیری منتخب

آسیب پذیری	نقطه ضعف	Base Score	Exploitability	Impact	Modified Base Score	M.Exploitability	Modified Impact
CVE-2016-6634	CWE-79	۶/۱	۲/۸	۲/۷	۴/۳۰۳۵	۰/۹۰۶۱	۳/۰۷۸۷
CVE-2016-6138	CWE-22	۹/۸	۳/۹	۵/۹	۶/۳۴۱۵	۰/۴۶۸۴	۵/۸۷۳۱
CVE-2016-2914	CWE-434	۵/۴	۲/۸	۲/۵	۳/۰۵۱۵	۰/۸۶۳۰	۲/۱۸۸۶
CVE-2016-4469	CWE-352	۸/۸	۲/۸	۵/۹	۷/۲۴۹	۱/۳۷۵۹	۵/۸۷۳۱
CVE-2016-4001	CWE-120	۶/۸	۲/۲	۴	۳/۸۵۲۸	۰/۸۱۵۱	۲/۷۵۲۳



شکل (۱): مدل پیشنهادی برای ارزیابی احتمال پویای زنجیره نقطه ضعف‌های امینتی

مراجع

[1] N.Idika, B.Bhargava, "Extending Attack Graph-based Security Metrics and Aggregating Their Application", IEEE Transactions on Dependable and Secure Computing, pp. 1-12, 2010.

[۲] مرجان کرامتی، "بررسی چالش‌های سیستم های الگوی حمله موجود و ارائه راهکار"، چهارمین کنفرانس بین المللی ترکیبیات، رمزنگاری، محاسبات و علوم کامپیوتر، ۸-۱دانشگاه علم و صنعت ایران، آبان ۹۸.

[3] M. Keramati, "Dynamic Risk Assessment System for the Vulnerability Scoring." International Journal of Information & Communication Technology Research, 9(4), 57-68, 2017.

[4] Microsoft Security Center , https://technet.microsoft.com/en-us/security/cc998259.aspx, , [Accessed September 2020].

[5] Symantec Vulnerability Scoring System , http://www.symantec.com/security_response/landing/vulnerabilities.jsp, , [Accessed September 2020].

[6] Redhat Vulnerability Scoring System , https://access.redhat.com/security/security-updates/#/, [Accessed September 2020].

[7] Common Vulnerability Scoring System (CVSS), https://www.first.org/cvss, , [Accessed September 2020].

[8] Santiago Figueroa-Lorenzo, Javier Añorga, and Saioa Arrizabalaga. 2020. A Survey of IIoT Protocols: A Measure of Vulnerability Risk Analysis Based on CVSS. ACM Comput. Surv. 53, 2, Article 44 (June 2020), 53 pages. DOI:https://doi.org/10.1145/3381038

[9] Carlos Cardoso Galhardo, Peter Mell, Irena Bojanova, and Assane Gueye. 2020. Measurements of the Most Significant Software Security Weaknesses. In Annual Computer Security Applications Conference (ACSAC '20). Association for Computing Machinery, New York, NY, USA, 154–164. DOI:https://doi.org/10.1145/3427228.3427257.

[10] Dimitriadis A, Flores JL, Kulvatunyou B, Ivezic N, Mavridis I. ARES: Automated Risk Estimation in Smart Sensor Environments. Sensors. 2020; 20(16):4617. https://doi.org/10.3390/s20164617

[11] Amankwah, R., Chen, J., Kudjo, P.K. et al. An automated framework for evaluating open-source web scanner vulnerability severity. SOCA 14, 297–307 (2020). https://doi.org/10.1007/s11761-020-00296-9

[12] F. Zhang and Q. Li, "Dynamic Risk-Aware Patch Scheduling," 2020 IEEE Conference on Communications and Network Security (CNS), Avignon, France, 2020, pp. 1-9, doi: 10.1109/CNS48642.2020.9162225.

[13] Saadatmand-Tarzjan M. A Novel Patch-Based Digital Signature. Journal of Iranian Association of Electrical and Electronics Engineers. 2019; 15 (4) :37-47

[14] Moghimi M, Akbaripour H, Amin-Naseri M R. Design of an Expert System to Detect Phishing Attacks in E-Banking. Journal of Iranian Association of Electrical and Electronics Engineers. 2015; 12 (2) :95-104

[15] Common Attack Pattern Enumeration and Classification (CAPEC), https://capec.mitre.org, Common Attack Pattern Enumeration and Classification (CAPEC), [Accessed September 2020].

[16] Common Weakness Enumeration (CWE), https://cwe.mitre.org, [Accessed September 2020].

[1] Rank