Journal of Information Technology Management
Vol. 9, No. 4
2017
DOI: 10.22059/jitm.2017.234709.2060

University of Tehran
Faculty of Management

Modeling and Simulation of Cyber Battlefield

Ali Jabar Rashidi [1], Mohammad Shakibazad [2]

Abstract: In order to protect cyberspace against cyber-attacks we need situation-specific cyber awareness framework for the implementation of our cyber maneuvers. This article allows an execution of cyber maneuvers providing dynamic cyber battlefield simulator. The proposed cyber battlefield contains essential information for the detection of cyber events; therefore, it can be considered as the most important and complicated factor in the high-level fusion. Cyber battlefield simulator provides detail of cyberspace elements including knowledge repository of vulnerability, tangible and intangible elements of cyberspace and the relationships between them that can_provide and execute cyber maneuvers, penetration test, cyber-attacks injection, attack tracking, visualization, cyber-attacks impact assessment and risk assessment. The dynamic maker Engine in simulator is designed to automatically update the knowledge base of vulnerabilities, to change the topology elements, and change the access list, services, hosts and users. Evaluation of simulator was done in a qualitative method of research and using a focus group.

Key words: ***Cyber battlefield, Cyber defense, Cyber situation awareness, Cyber space simulator, Modeling.***

1. Associate Prof. in Eelectrical Engineering at Malek Ashtar University of Technology, Tehran, Iran
2. Ph.D. Candidate of Information Technology Management, Malek Ashtar University of Technology, Tehran, Iran

Submitted: 01 / June / 2017
Accepted: 20 / September / 2017
Corresponding Author: Ali Jabar Rashidi
Email: aiorashid@yahoo.com

مدیریت فناوری اطلاعات
دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۹، شمارهٔ ۴
زمستان ۱۳۹۶
صص. ۸۲۸- ۸۰۹

Journal of Information Technology Management
DOI: 10.22059/jitm.2017.234709.2060

مدل‌سازی و شبیه‌سازی صحنهٔ نبرد سایبری

علی جبار رشیدی[۱]، محمد شکیبازاد[۲]

چکیده: به‌منظور حفاظت از فضای سایبری و مقابله با حملات آن، به چارچوب آگاهی وضعیتی سایبری برای اجرای مانورهای آن نیاز داریم. پژوهش پیش رو چالش‌های اجرای این مانورها را با شبیه‌سازی پویای صحنهٔ نبرد سایبری رفع می‌کند. صحنهٔ نبرد ارائه‌شده حاوی اطلاعات ضروری برای تشخیص رخدادهای سایبری است، از این رو می‌توان آن را به‌عنوان مهم‌ترین و پیچیده‌ترین عامل در ادغام سطح بالا در نظر گرفت. صحنهٔ نبرد سایبری حاوی اطلاعات دقیقی از عناصر محیط سایبری، شامل مخزن دانش آسیب‌پذیری، اجزای ملموس و ناملموس محیط سایبری و روابط بین آنهاست که امکان اجرای مانور، آزمون نفوذ، تزریق حملات سایبری، ردیابی حملات، مصورسازی، ارزیابی اثر حملات سایبری و ارزیابی ریسک را فراهم می‌کند. موتور پویاساز شبیه‌ساز، به‌منظور به‌روزرسانی خودکار پایگاه دانش آسیب‌پذیری، تغییر توپولوژی و ویژگی‌های عناصر، دسترسی‌ها، سرویس‌ها، میزبان‌ها و کاربران طراحی شده است. به‌کمک روش تحقیق کیفی و همچنین با ایجاد گروه کانونی، مدل‌سازی و شبیه‌سازی ارزیابی شده است.

واژه‌های کلیدی: آگاهی وضعیتی سایبری، دفاع سایبری، شبیه‌ساز فضای سایبری، صحنهٔ نبرد سایبری، مدل سازی.

۱. دانشیار گروه برق و مخابرات، دانشکدهٔ برق، دانشگاه صنعتی مالک اشتر، تهران، ایران
۲. دانشجوی دکتری مهندسی فناوری اطلاعات و امنیت، دانشکدهٔ فناوری اطلاعات ارتباطات و امنیت، دانشگاه صنعتی مالک اشتر، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۶/۰۳/۱۱
تاریخ پذیرش نهایی مقاله: ۱۳۹۶/۰۶/۲۹
نویسندهٔ مسئول مقاله: علی جبار رشیدی
E-mail: aiorashid@yahoo.com

مقدمه

با افزایش پیچیدگی فضای سایبری، پیچیدگی دفاع در برابر حملات آن افزایش یافته است. حملات سایبری می‌توانند در شبکه‌های نظامی و همچنین زیرساخت‌های شبکه‌ای غیرنظامی پیامدهای ناگواری ایجاد کنند (نیروی هوایی آمریکا، ۲۰۱۲). ماهیت جنگ‌ها از حوزهٔ نظامی به سایبری تغییر پیدا کرده است. در این حملات از طریق فضای مجازی به زیرساخت‌های مهم کشور از راه دور حمله می‌شود. آنچه یک مهاجم با نفوذ به مرزهای سایبری دیگران به‌دست می‌آورد، از خاک و اشغال سرزمین بسیار ارزشمندتر است. خطر حملات سایبری کمتر از اقدام نظامی نیست و برای هر دولتی پیامدها و اثرهای مرگباری به‌دنبال دارد. به همین دلیل، توجه ویژه به این حوزه ضروری است. ایران یکی از بزرگ‌ترین قربانیان تهاجم سایبری در جهان است. تولید دانش بومی در این حوزه اهمیت شایان توجهی دارد. ارزشمندترین دارایی هر سازمان که باید از آن محافظت شود، اطلاعات، به‌خصوص اطلاعات مالی و بانکی است (عرب‌سرخی، موسی‌خانی و مانیان، ۱۳۹۵؛ حاج‌ملک و توکلی، ۱۳۹۵ و ونکی، تقوا، تقوی فرد و فیضی، ۱۳۹۶). در اسناد بالادستی در حوزهٔ امنیت سایبری کشورها بر وجود یک مدل بومی در امنیت سایبری تأکید شده، زیرا امنیت سایبری بخش مهمی از امنیت ملی محسوب می‌شود.

سازمان‌ها به زیرساخت‌های فناوری اطلاعات و محیط سایبری وابستگی شدیدی دارند و نفوذ، خرابکاری و افشای اطلاعات سازمان‌ها هزینه‌های زیادی در پی خواهد داشت، در نتیجه امن‌سازی این محیط بسیار ضروری است. یکی از مسائل در شناسایی نقاط آسیب‌پذیر شبکه، نرم‌افزارها و سخت‌افزارهایی است که در محیط سایبری وجود دارد. به‌دلیل مشکلات اجرایی آزمون نفوذ مانند هزینه‌بر بودن، احتمال ایجاد اختلال در سرویس‌دهی و عدم اعتماد کامل به شرکت‌های اجراکنندهٔ آزمون نفوذ، ارائهٔ راهکاری به‌منظور اجرای مانورهای سایبری خارج از محیط واقعی و فیزیکی در سازمان‌ها، یک ضرورت است.

برای دفاع سایبری، سامانهٔ آگاهی وضعیتی‌ای لازم است تا از وضعیت اجزای محیط سایبری، اطلاعات کامل و دقیقی در اختیار تحلیلگر قرار دهد. هدف این پژوهش ارائهٔ ابزارهای دفاع فضای سایبری مبتنی بر آگاهی وضعیتی است، به‌گونه‌ای که به تصمیم‌گیری درست و به‌موقع برای مقابله با حملات سایبری منجر شود. با توجه به اینکه تاکنون مدل جامعی برای این حوزه ارائه نشده، باید در این خصوص مدلی بومی طراحی شود.

پیشینهٔ پژوهش

در این بخش به مفاهیم پایهٔ تحقیق شامل آگاهی وضعیتی سایبری، آسیب‌پذیری‌ها، محیط سایبری، مدل و در نهایت بررسی ادبیات موضوعی پرداخته خواهد شد.

پیشینهٔ نظری

آگاهی وضعیتی: آگاهی وضعیتی، آگاهی از آن چیزی است که در فضای سایبری و محیط اطراف آن رخ می‌دهد و فرایندی شناختی است که می‌تواند شرایط حال حاضر فضای سایبری را درک کرده و پس از فهم معنای آن، تصمیم‌گیری کند. آگاهی وضعیتی از سه سطح دریافت، تفسیر (فهم) و تجسم یا پیش‌بینی تشکیل شده است (اندسلی و اریک، ۲۰۱۴). در مقالهٔ آشتیانی و ازگومی (۲۰۱۴) شبیه‌سازی حملات سایبری با رویکرد توزیع‌شدگی ارائه شده است. توزیع‌شدگی به‌وجود آوردن امکان تعامل میان افراد و برنامه‌ها در مکان‌های جغرافیایی مختلف است. این شبیه‌ساز در دو حالت تحلیلی و تعاملی قابل اجرا است که برای شناخت برخی ضعف‌های شبکه، از آن استفاده می‌شود.

آسیب‌پذیری: طبق تعریف ENISA آسیب‌پذیری وجود ضعف یا خطا در طراحی یا پیاده‌سازی است که می‌تواند به رویداد ناگهانی و نامطلوب منجر شود و باعث به خطر انداختن امنیت و نقض سیاست‌های امنیتی سامانه، شبکه، نرم‌افزار یا پروتکل می‌شود. نفوذ با سوءاستفاده از آسیب‌پذیری‌ها صورت می‌گیرد (حبیبی، علیزاده و مشکینی، ۲۰۱۳). در نتیجه یکی از داده‌های پایه‌ای در مدل‌سازی و شبیه‌سازی، صحنهٔ نبرد سایبری است.

مدل: مدل یا الگو، نمونهٔ ساده‌شده‌ای از واقعیت است. الگوها و مدل‌ها می‌توانند شامل تصویرهای ذهنی، نمایش‌های گرافیکی، نمایش‌های بیانی یا نمایش‌های ریاضی از واقعیت باشند. در نتیجه الگوها و مدل‌ها به تصویر ایستای واقعیت، اشاره‌ای ضمنی می‌کنند (لطفیان، ۱۳۷۶).

محیط سایبری: هر محیطی از جمله محیط سایبری، حاوی اجزا و المان‌هایی است. عناصر صحنهٔ نبرد سایبری شامل اجزای ملموس، ناملموس و ارتباطات میان آنان است (شکیبازاد و رشیدی، ۲۰۱۷).

پیشینهٔ تجربی

گراف‌های حمله: گراف حمله امکان نفوذ از یک نقطهٔ شروع مشخص به شبکهٔ کامپیوتری را مشخص می‌کند. در پژوهش فلیپس و سویلر (۱۹۹۸) از گراف حمله برای ارزیابی آسیب‌پذیری‌ها

استفاده شده است. لیپمن و اینگولز (۲۰۰۵) بررسی جامعی در مورد گراف‌های حمله انجام داده‌اند. گراف‌های حمله، گراف‌های بدون دوری است که نشان‌دهندهٔ گام‌های مختلف و ممکن برای یک حمله است. در اغلب پیاده‌سازی‌ها، هر گراف می‌تواند فقط یک هدف را مدل کند، اما برخی از آنها می‌توانند در یک گراف چند هدف را مدل کنند. طبق نظر لیپمن و اینگولز (۲۰۰۵) یکی از مشکلات پیاده‌سازی مدل گراف‌های حمله است. از آنجا که این گراف‌ها مدور نیستند، در یک گراف حمله نمی‌توان ارتباط دوطرفهٔ بین میزبان‌ها را مدل کرد، از این رو برای مدل کردن این ارتباطات لازم است گراف‌های متعددی ایجاد شود و برای چندین هدف باید چندین گراف حمله ایجاد شود. از آنجا که صحنهٔ نبرد سایبری محدودیت بدون دور ندارد، مشکل گراف‌های حمله را نخواهد داشت؛ یعنی همهٔ انتقال‌ها می‌تواند فقط در یک صحنه مدل شود. از دلایل دیگر شکست گراف‌های حمله، فرض کردن ارتباط ایستا بین گره‌هاست. با توجه به دیوار آتش و مسیریاب‌ها، از آنجا که ترافیک‌های مختلف بین دو میزبان مجاز یا غیرمجاز ایجاد می‌شود، نمی‌توان چنین فرضی داشت. این چالش نیز در مدل پیشنهادی پوشش داده شده است. در مدل صحنهٔ نبرد سایبری، قوانین دیوارآتش و فهرست دسترسی‌ها در نظر گرفته شده است. از این رو برای تشخیص مجاز بودن ترافیک، اطلاعات لازم وجود دارد.

درخت آسیب‌پذیری: درخت آسیب‌پذیری در واقع گراف حمله‌ای است که مانند یک درخت مدل شده است. ریشهٔ درخت، هدف نهایی حمله است؛ برگ‌ها نقاط شروع منطقی و گره‌های دیگر مراحل مختلف حمله را نشان می‌دهند. پیمایش از یک گرهٔ برگ درخت به ریشه، نشان‌دهندهٔ دنباله‌ای ممکن از حملات است. هر گره پیچیدگی‌ای دارد که میزان پیچیدگی اجرای حمله را نشان می‌دهد. ویدالیس و جونز (۲۰۰۳) در پژوهشی به‌کمک درختان آسیب‌پذیری، تلاش کردند آسیب‌پذیری را ارزیابی کنند. در پژوهش اسچینر (۱۹۹۹) از درخت آسیب‌پذیری برای ارتقای امنیت استفاده شده است. درختان آسیب‌پذیری مانند گراف‌های حمله با چالش مقیاس‌پذیری روبه‌رو هستند. از آنجا که یک درخت آسیب‌پذیری برای رسیدن به یک هدف تعریف می‌شود، برای چندین هدف باید چندین درخت آسیب‌پذیری تعریف کرد. این شیوهٔ تعریف، درخت آسیب‌پذیری را برای یک شبکهٔ بزرگ بسیار دشوار می‌کند، زیرا به تعریف تعداد زیادی درخت آسیب‌پذیری بزرگ و پیچیده نیاز داریم. این مشکل در مدل پیشنهادی صحنهٔ نبرد سایبری رفع شده و به‌طور ضمنی قادر به مدل کردن تمام حملات مشخص و اهداف شناخته‌شده در یک مدل واحد است.

مقیاس‌پذیری صحنهٔ نبرد سایبری، فقط به مقیاس‌پذیری الگوریتم‌های به‌کار رفته در تحلیل صحنهٔ نبرد سایبری وابسته است. در درخت آسیب‌پذیری مانند گراف حمله، ارتباطات بین

میزبان‌ها ایستا فرض شده و قوانین دیوار آتش لحاظ نشده است. تعریف یک حملهٔ جدید یا تغییر در پیکربندی شبکه، می‌تواند باعث تغییر چشمگیری در ساختار درخت آسیب‌پذیری شود. از آنجا که تغییرات شبکه یا نوع حمله یا قوانین دیوار آتش به تغییرات کوچکی در مدل صحنهٔ نبرد سایبری می‌انجامد، مراحل حمله توسط صحنهٔ نبرد سایبری به‌صراحت مدل نمی‌شود.

در مقالهٔ یانگ، هلسپل و لویی (۲۰۰۹) ارزیابی اثر و پیش‌بینی تهدید به کمک نمونه‌سازی تشریح و مقایسه شده است. در این پژوهش ارزیابی اثر به‌منظور تخمین میزان خسارت‌های ناشی از حمله ارائه شده که ضرایب حساسیت در این پژوهش در نظر گرفته نشده است. کنتکو و چچولینگ (۲۰۱۳) در پژوهشی، چارچوبی را برای مدل‌سازی حملات سایبری با استفاده از گراف حمله و ارزیابی اثر ارائه کرده‌اند. در این پژوهش برای توصیف و ارزیابی نحوهٔ عملکرد مدل از نمونه‌سازی استفاده شده است. آنها در کار خود از روش‌های تحلیل رویداد بی‌درنگ، پیش‌بینی مراحل آیندهٔ حمله و ارزیابی اثر حمله برای تحلیل و ساخت گراف حمله استفاده کرده‌اند. ضعف اصلی این پژوهش مربوط به مشکلات مقیاس‌پذیری گراف‌های حمله است. ویلر (۲۰۱۴) مدلی برای شبکهٔ کامپیوتری، به‌منظور ارزیابی سازوکارهای دفاعی شبکه با اهداف در حال حرکت ارائه کرده‌اند. هدف از این مدل‌سازی تغییر ویژگی‌های شبکه به‌منظور گمراه کردن نفوذگر است. آنها از روش‌های تغییر پویای آدرس IP، تغییر پویای پورت و دیوار آتش پویا در محیط شبیه‌ساز حمله سایبری استفاده کردند. موسکال، ویلر، کریجر، کوهل و یانگ (۲۰۱۴) با ادغام مدل مفهومی، حملات چند مرحله‌ای شبکه را شبیه‌سازی کرده است. شبیه‌ساز وی با عنوان MASS، به مدل‌سازی شبکه، ساختار سلسله‌مراتبی آسیب‌پذیری، رفتار حمله و سناریوی حمله پرداخته است. در پژوهش هلسپل، سودیت و یانگ (۲۰۱۵)، روی ارزیابی اثر حملات سایبری در شبکهٔ کامپیوتری تحقیق شده است. آنان به پژوهش‌های قبلی در این خصوص نیز اشاره کرده‌اند. در جدول ۱ پیشینهٔ تجربی مقایسه شده است.

یکی از ابزارهای ارائه‌شده در حوزهٔ امنیت سایبری SOC است. این ابزار با جمع‌آوری همبسته‌سازی و ادغام هشدارها از حسگرهای امنیتی، حملات احتمالی را شناسایی می‌کند. کارایی این ابزار صرفاً در حین انجام حمله یا بعد از وقوع حمله است و چون امکان تزریق حملات و شبیه‌سازی در این ابزارها وجود ندارد، نمی‌تواند برای اقدام‌های پیشگیرانه، امن‌سازی و مانور استفاده شود. نگوین، علی و یو (۲۰۱۶)، در بخشی از مقالهٔ مروری خود با مطرح کردن چالش و محدودیت عدم امکان اعتبارسنجی و صحت‌سنجی، آن را نشان‌دهندهٔ جدید بودن و نابالغ بودن این حوزه دانستند.

جدول ۱. پیشینهٔ تجربی

سال	پژوهشگر	کارهای انجام‌شده	ویژگی‌ها	مدل آسیب‌پذیری	شبیه‌سازی	پشتیبانی از مدل آگاهی وضعیتی	مولد خودکار تصویر شبکه	ارزیابی اثر یا ریسک
۱۹۹۸	فلیپس و سویلر	تحلیل ریسک با شبکهٔ بیزین	گراف بدون دور	درخت آسیب‌پذیری	واسط ندارد	ندارد	ندارد	ندارد
۲۰۰۹	یانگ، هلسپل و همکاران	ارزیابی اثر و پیش‌بینی تهدید	تخمین خسارت با نمونه‌سازی	ندارد	واسط ندارد	دارد	ندارد	دارد
۲۰۱۳	کنتکو، چچولینگ	چارچوبی برای مدل‌سازی حملات سایبری و ارزیابی اثر	ایجاد گراف حمله، مدل‌سازی حمله	ندارد	دارد	ندارد	ندارد	دارد
۲۰۱۴	ویلر و فردریک	مدل‌سازی شبکه با قابلیت گمراه کردن نفوذگر	تغییر پویای آدرس IP، تغییر پویای پورت و دیوارآتش پویا	ندارد	واسط ندارد	ندارد	ندارد	ندارد
۲۰۱۴	ویلر و همکاران	مدل‌سازی شبکه، ساختار سلسله‌مراتبی آسیب‌پذیری، رفتار حمله و سناریوی حمله	ترکیب مدل شبکه، ساختار آسیب‌پذیری، رفتار حمله و مدل حمله برای شبیه‌سازی حملات چندمرحله‌ای	دارد	واسط ندارد	دارد	ندارد	ندارد
۲۰۱۵	هلسپل و همکاران	مروری بر موتور ادغام و مدل‌سازی شبکه و ارزیابی اثر	ارائهٔ زیرسیستم‌های مورد نیاز برای ارزیابی اثر	ندارد	واسط ندارد	دارد	ندارد	دارد

نوآوری این پـژوهش ارائـهٔ مـدل صـحنهٔ نبـرد سـایبری یکپارچـه، شـامل مـدل سـرویس، آسیب‌پذیری، میزبان، شبکه و الگوریتم‌ها (ارزیابی ریسـک، امتیازهـای اثـر، ضـرایب حساسـیت، منطقی بودن حمله) برای تزریق حملات و تحلیل‌های امنیتی اسـت. موتـور پویاسـاز صـحنه در محور زمان وظیفهٔ پویاسازی و توسعهٔ بی‌درنگ صحنه را دارد. نمایش گرافیکی تحلیلی‌ها شـامل نمودارهای ارزیابی اثر حمله و ردیابی میسر حملـه روی توپولـوژی شـبکه اسـت و داشـبوردهای مدیریتی، وضعیت فعلی صحنه به‌منظور دستیابی به آگاهی وضعیتی سایبری را نمایش می‌دهند.

زمانی که یک آسیب‌پذیری شناسایی و ثبت می‌شود، مدتی طول می‌کشد تـا در رسـانه‌هـای امنیتی اطلاع‌رسانی شود. بخش زیادی از نفوذها در ایـن بـازهٔ زمـانی رخ مـی‌دهـد کـه در ایـن پژوهش این مسئله رفع شده است.

یکی از مسائل حوزهٔ امنیت اطلاعات، نبود ابزاری برای ارائهٔ راهکارهای امنیتی برای ارتقـای سطح امنیت کل شبکه است. با توجه به اینکه خرید تجهیزات امنیتی، تجهیزات شبکه، خریـد یـا ارتقای نرم‌افزارها و تغییر پیکره‌بندی شبکه، هزینهٔ مالی و زمانی زیادی دارد، طرح صحنهٔ نبرد بـا تحلیل‌های امنیتی‌ای که از طریق تزریق انواع حملات انجام می‌دهد، می‌تواند به مدیر شبکه برای ارتقای سطح امنیت شبکه، اولویت‌بندی و پیشنهادهایی ارائه دهد.

با توجه به بررسی‌های انجام‌شده، در این حوزه مقاله‌های مرتبط بسیار محـدودی وجـود دارد. پژوهش‌ها و فعالیت‌های انجام‌شده در حوزهٔ نظامی و امنیت سایبری طبقه‌بندی شده‌انـد. یکـی از محدودیت‌ها نبود دادگان و مقاله‌های مرتبط به دلایل محرمانه است. نگوین، علی و یـو (۲۰۱۶)، در بخشی از مقالهٔ مروری خود با مطرح کردن چالش و محـدودیت عـدم امکـان اعتبارسـنجی و صحت‌سنجی، آن را نشان‌دهندهٔ جدید بودن و نابالغ بودن این حوزه دانستند.

همان‌طور که در مبانی نظری بیان شد، در مقاله‌های مختلف این حـوزهماننـد مقالـهٔ یانـگ، هلسپل و لویی (۲۰۰۹) و کنتکو و چچولینگ (۲۰۱۳) به‌منظور مقایسه و ارزیابی عملکرد مدل، از نمونه‌سازی استفاده شده است؛ از این رو در مقالهٔ حاضر نیز از روش نمونه‌سـازی و شـبیه‌سـازی استفاده شده است.

روش‌شناسی پژوهش

روش شیء‌گرا قابلیت مدل‌سازی پدیده‌های دنیـای واقعـی را فـراهم مـی‌کنـد. در واقـع محـیط سایبری را به‌صورت مجموعه‌ای از اشیا، صفات، رفتار، فرایندها، ارتباطات و تعامل‌های داده‌ای به ما نشان می‌دهد. از روش شیء‌گرا برای مدل‌سـازی اجـزای فیزیکـی، غیرفیزیکـی، ارتباطـات و فرایندها، ایده گرفته شده است؛ در نتیجه طرح به‌گونه‌ای اجرا مـی‌شـود کـه در مقابـل تغییـرات

اطلاعاتی و رفتاری انعطاف‌پذیر باشد. در پیاده‌سازی شبیه‌ساز نیز از همین روش استفاده شده است.

روش ارزیابی مدل

زمانی که به داده‌های کیفی/ تفصیلی دربارهٔ نظر افراد راجع به پدیده‌ای نیاز است، می‌توان از رویکرد گروه‌های کانونی استفاده کرد. پژوهشگرانی که روش پژوهش توصیفی ـ پیمایشی را به‌کار می‌برند، می‌توانند پس از گردآوری داده‌های کمی، برای تفسیر نتایج به‌دست آمده از داده‌ها، از این روش استفاده کنند. به‌منظور ارزیابی، بررسی و اثبات صحت مدل‌سازی و میزان دقت آن، از روش تحقیق کیفی گروه کانونی استفاده شده است. ابتدا مدل‌سازی در گروه کانونی ارزیابی می‌شود؛ سپس با شبیه‌سازی، صحت عملکرد مدل در گروه کانونی تحلیل و سنجش خواهد شد (بازرگان، ۲۰۱۰).

با توجه به اینکه هدف، تحلیل‌های امنیتی روی شبکهٔ سازمان‌های بزرگ است، باید برای نمونه‌سازی واقعی، شبکهٔ بزرگ و نسبتاً پیچیده‌ای به پراکندگی کل کشور با سطح امنیتی نسبتاً زیاد و سرویس‌های متنوع انتخاب شود. از این رو پروژهٔ کارت هوشمند سوخت که در کلیهٔ جایگاه‌های سوخت، دفاتر پلیس ۱۰+، دفاتر پست و مناطق و نواحی شرکت ملی پخش فراورده‌های نفتی ایران وجود دارد، انتخاب شد. با توجه به اینکه پس از ۱۰ سال از راه‌اندازی این سامانه، هیچ مهاجمی نتوانسته به این شبکه نفوذ کند، می‌توان نتیجه گرفت که نمونهٔ انتخابی هم اکنون از سطح امنیتی مطلوبی برخوردار است. یکی از حملات سایبری به شرکت ملی پخش فراورده‌ای نفتی در سال ۱۳۹۱ انجام شد (اسفندیارپور و اکبری، ۲۰۱۶) که شبکه و طرح ملی سامانهٔ هوشمند سوخت از این حمله مصون ماند.

از سویی لازم است خبرگان از جامعه‌ای انتخاب شوند که در حوزهٔ امنیت اطلاعات از تخصص کافی و سابقهٔ چندسالهٔ فعالیت برخوردار باشند. این افراد باید در پیاده‌سازی شبکه‌های گسترده و پیچیده در سطح ملی تجربهٔ کاری داشته باشند. با توجه به حائز شرایط بودن شبکهٔ کارت هوشمند سوخت، از کارشناسان خبره و فعال در حوزهٔ امنیت این پروژه برای همکاری دعوت شد. شبکهٔ نمونهٔ انتخابی در شبیه‌ساز صحنهٔ نبرد، پیاده‌سازی شد و نتایج شبیه‌ساز با نتایج واقعی حاصل از تجهیزات امنیتی مقایسه گردید. گروه کانونی از شش نفر خبرهٔ حوزهٔ سایبری و امنیت شبکه با حداقل مدرک کارشناسی ارشد و سابقهٔ پنج سال، از میان کارمندان فنی سامانهٔ هوشمند سوخت تشکیل شد. درصد خطای قابل قبول برای الگوریتم‌ها حداکثر ۱۵ درصد در نظر گرفته شد و با این معیار، بهینه‌سازی الگوریتم‌ها تا رسیدن به نتیجهٔ مطلوب صورت گرفت. در هر جلسه، نتایج بررسی و مقایسه شدند و با مشارکت تمام گروه، انحراف‌ها شناسایی شده و بعد از

اعمال اصلاحات برای بررسی نتایج، جلسه بعدی تشکیل می‌شد. طی یک ماه چهار جلسه برگزار شد تا گروه دربارهٔ نتایج توافق کنند. سؤال‌های طرح‌شده در گروه کانونی به شرح زیر است.

ارزیابی مدل‌سازی و سنجش میزان دقت: آیا مدل‌سازی صورت‌گرفته مدل مناسبی برای فضای سایبر با هدف تحلیل‌های امنیتی است؟ آیا مدل به‌وجودآمده برای ایجاد شبیه‌سازی صحنهٔ نبرد سایبری به‌اندازهٔ کافی مناسب است؟

سنجش کامل بودن و جامعیت مدل: آیا اجزای در نظر گرفته‌شده در مدل شبکه، مدل سرویس، مدل آسیب‌پذیری و در نتیجه مدل صحنهٔ نبرد سایبری عناصر مورد نیاز برای محیط سایبری را دربردارند و این اجزا از جامعیت کافی برخوردارند؟ آیا عناصر در نظر گرفته شده برای تحلیل‌های امنیتی شامل تحلیل‌های هوش تجاری، داده‌کاوی، ارزیابی اثر و ارزیابی ریسک مناسب انتخاب شده است؟

بررسی قابلیت توسعه‌پذیری و کوچک‌سازی صحنه: با توجه به ماهیت فضای سایبری ویژگی توسعه‌پذیری از الزامات این پژوهش است. آیا امکان توسعه‌پذیری و کوچک‌سازی صحنه در نظر گرفته شده است؟ آیا امکان توسعه‌پذیری و کوچک‌سازی شامل اضافه و حذف اجزا از محیط و ایجاد تغییرات بر ویژگی اجزا به‌درستی طراحی و پیاده‌سازی شده است؟ آیا امکان ویرایش مجوزهای دسترسی بین میزبان‌ها، قوانین دسترسی روی دیوار آتش، ویرایش سرویس‌های هر میزبان و ویرایش میزبان‌های صحنه به‌درستی طراحی و پیاده‌سازی شده است؟

بررسی الگوریتم‌های ارزیابی ریسک، ارزیابی اثر و میزان حساسیت عناصر: آیا الگوریتم استفاده‌شده برای اندازه‌گیری امتیاز اثر هر گام حمله‌بر روی سرویس، میزبان، کاربر و کل شبکه عملکرد و نتایج درستی داشته است؟ آیا روش ارزیابی ریسک استفاده‌شده برای سرویس‌ها، میزبان‌ها، کاربران و کل شبکه به‌درستی انتخاب شده است؟ آیا میزان حساسیت هر سرویس، میزبان و محدوده به‌درستی انتخاب شده است؟

برای ارزیابی الگوریتم‌ها با شبیه‌سازی بخشی از شبکهٔ سامانهٔ کارت هوشمند سوخت، خروجی الگوریتم‌ها با نتایج به‌دست‌آمده از ابزارهای امنیتی و نرم‌افزارهای تحلیلی، مقایسه شد و نتایج برای بررسی در اختیار گروه کانونی قرار گرفت. نمونه‌ای از گزارش اصلاحات اعلامی به این شرح بود: پارامترهای ساختار سلسله‌مراتبی باید کامل‌تر شود. مدل معماری کلان صحنه نیاز به اصلاح دارد. پارامترهای الگوریتم‌های حساسیت، ارزیابی اثر و ریسک باید وزن‌دهی شوند.

فرایندهای صحنه باید ترسیم و تشریح شوند. پایگاه دادهٔ مکانی به صحنه اضافه شده و آسیب‌پذیری‌ها به‌صورت خودکار به‌روز شود.

با توجه به دریافت بازخورد از گروه کانونی، اصلاحات لازم در بخش‌های مدل‌سازی و شبیه‌سازی صورت پذیرفت و طی جلسهٔ بعدی نتایج بازبینی شدند. بعد از برگزاری چند جلسه و اعمال اصلاحات، گروه کانونی پوشش تمام موارد مطرح‌شده را تأیید کرد.

یافته‌های پژوهش

معماری کلان صحنهٔ نبرد سایبری پویا

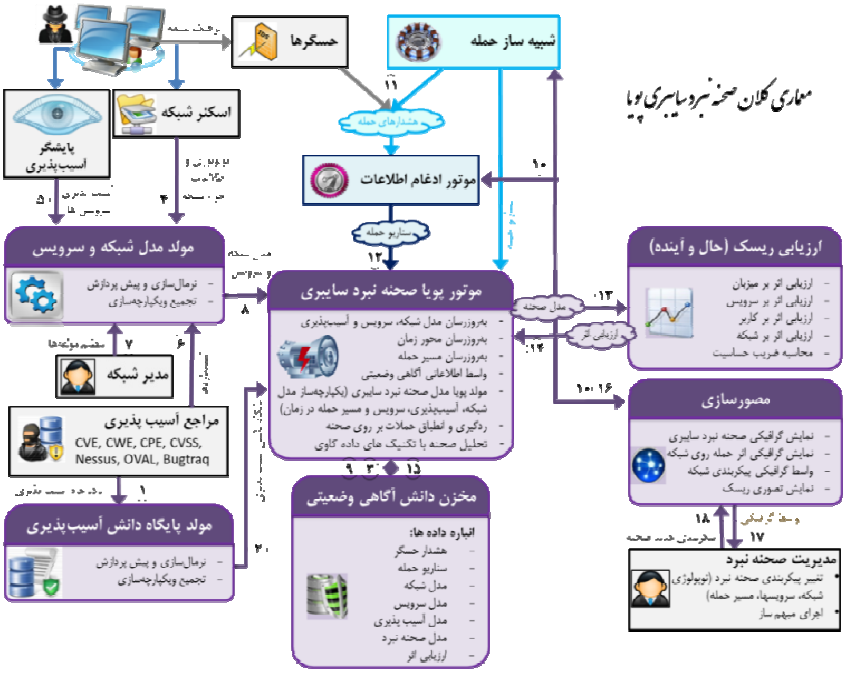
معماری کلان صحنهٔ نبرد سایبری پویا در ۰شکل ۱ نمایش داده شده است. برای دستیابی به آگاهی وضعیتی سایبری ابتدا باید از وضعیت فعلی محیط شناخت کافی داشته باشیم و لازم است مشخصات اجزای محیط و سپس آسیب‌پذیری‌های هر یک از اجزا را شناسایی کنیم. صحنهٔ نبرد سایبری برای اجرای مانورهای خود به دو سامانهٔ بیرونی شامل شبیه‌ساز حملات سایبری و موتور ادغام اطلاعات سایبری نیاز دارد.

در صورتی که بخواهیم مانور سایبری را در محیط غیرعملیاتی انجام دهیم، هشدارهای حمله (یا به‌صورت مستقیم سناریوی حمله) توسط شبیه‌ساز حمله تولید شده و به صحنهٔ نبرد تزریق می‌شود و در ادامه اثر و ریسک ارزیابی می‌شوند. در این شرایط می‌توان به‌طور خودکار انواع مختلف حملات با ویژگی‌های مختلف را در صحنه تزریق کرد و در ادامه با تحلیل نتایج به‌دست‌آمده می‌توان ضعف‌ها و آسیب‌پذیری‌های موجود در محیط سایبری را شناسایی نمود. مدیر صحنه به کمک این تحلیل‌ها می‌تواند با تغییر پیکربندی شبکه، اقدام‌های لازم برای امن‌سازی فضای سایبری را در محیط شبیه‌ساز انجام دهد. بعد از اعمال پیکره‌بندی جدید در مرحلهٔ بعد مدیر شبکه با تزریق حملات گسترده‌تر میزان مقاومت صحنه را ارزیابی می‌کند. در این شرایط می‌توان پیش‌بینی کرد، چه پیکربندی امنیتی می‌تواند بیشترین سطح مقاومت را برای محیط سایبری فراهم آورد. در ادامه، زیرسیستم‌های صحنهٔ نبرد سایبری معرفی شده‌اند.

مولد مدل شبکه و سرویس

محیط سایبری شامل اجزای ملموس، ناملموس و ارتباطات میان آنها است. اجزای ملموس اجزایی مانند ایستگاه‌های کاری، سرورها، کاربران، دیوارهای آتش، مسیریاب‌ها، سامانه‌های تشخیص و جلوگیری از نفوذ هستند. این اطلاعات توسط اسکنرهای شبکه و فایل‌های پیکربندی از محیط شبکه گردآوری می‌شود. سرویس، خوشهٔ میزبان، پروتکل، آسیب‌پذیری و سناریوی حملات اجزای ناملموس‌اند. ارتباطات اجزای صحنه نیز، فهرست دسترسی بین اجزا و

قوانین دیوار آتش است. پیش‌پردازش و یکپارچه‌سازی این اطلاعات توسط این زیرسامانه انجام می‌شود و در گام بعد بر اساس استانداردها، نرمال‌سازی اطلاعات انجام می‌شود و در نهایت توسط مدیر شبکه امکان نظارت و تکمیل اطلاعات توپولوژی شبکه وجود دارد.



شکل ۱. معماری کلان صحنهٔ نبرد سایبری پویا (یافتهٔ تحقیق)

مولد پایگاه‌دانش آسیب‌پذیری

آسیب‌پذیری‌های کشف‌شده در فضای سایبری روزانه در چند مرجع اصلی ثبت می‌شود. در کنار این مراجع، برای طبقه‌بندی و امتیازبندی آسیب‌پذیری‌ها، استانداردهایی ایجاد شده که برای درک وضعیت فعلی محیط سایبری به این اطلاعات نیاز داریم. مولد پایگاه دانش آسیب‌پذیری با تجمیع، همبسته‌سازی و دسته‌بندی آسیب‌پذیری‌ها، فرایند را ایجاد کرده و به‌روزرسانی را انجام می‌دهد. هر سرور یا ایستگاه کاری در محیط سایبری شامل چندین سرویس فعال است که می‌توانند حاوی آسیب‌پذیری‌هایی باشند. شناسایی آسیب‌پذیری سرویس‌ها و سایر اجزای صحنهٔ نبرد توسط موتور پویای صحنه صورت می‌گیرد.

حل مسئلهٔ شناسایی خودکار و لحظهٔ آسیب‌پذیری‌ها و اعلام آن در محیط سایبری در این بخش انجام می‌شود. در مرحلهٔ نخست کل آسیب‌پذیری‌های ثبت‌شده از مراجع ثبت آسیب‌پذیری

گردآوری شده و با انجام پردازش‌های لازم و برقراری ارتباط میان سرویس‌ها در پایگاه دانش ذخیره‌سازی می‌شود. در ادامه توسط یک عامل و ربات خودکار و برخط در بازه‌های زمانی کوتاه مراجع ثبت آسیب‌پذیری در اینترنت بررسی شده و در صورت نیاز به‌روزرسانی انجام می‌شود. در صورتی که آسیب‌پذیری جدیدی شناسایی شود و همچنین در صحنهٔ نبرد مد نظر از سرویس‌های تحت تأثیر آن آسیب‌پذیری استفاده شده باشد، به مدیر صحنه برای برطرف‌سازی سریع مشکل یا قطع موقت سرویس تا زمان رفع مشکل، هشدارها و اطلاعات لازم داده می‌شود.

موتور پویای صحنهٔ نبرد سایبری

این زیرسامانه به‌عنوان هستهٔ اصل صحنهٔ نبرد با دریافت اطلاعات مدل شبکه، مدل سرویس، پایگاه‌دانش آسیب‌پذیری و سناریوی حملهٔ فرایند ایجاد صحنهٔ نبرد سایبری، پویاسازی صحنه، ردگیری، انطباق حملات و تحلیل‌های آماری صحنه را انجام داده و همچنین به‌عنوان واسط اطلاعاتی آگاهی وضعیتی برای تبادل اطلاعات در قالب استاندارد عمل می‌کند.

مصورسازی

مصورسازی در راستای نمایش گرافیکی توپولوژی و اجزای صحنه (میزبان، کاربر، سرویس، دیوارآتش و ارتباط‌های فیزیکی میان اجزا)، نمایش گرافیکی بی‌درنگ رد حمله، نمایش گرافیکی اثر هر گام حمله‌بر روی اجزای صحنه، نمایش نمودارها و تحلیل‌های آماری از جمله ارزیابی اثر و ریسک، نمایش گرافیکی وضعیت اجزا (فعال و عادی، غیرفعال، هک‌شده) استفاده می‌شود. با توجه به ماهیت پویای صحنه، باید اثر هر تغییر به صورت گرافیکی و بی‌درنگ در صحنه به‌روزرسانی شود.

مخزن دانش آگاهی وضعیتی

اطلاعات اجزای صحنه به‌منظور استفادهٔ الگوریتم‌ها لازم است تجمیع، پیش‌پردازش، نرمال‌سازی، یکپارچه‌سازی و نهایتاً در مخزن دانش، آگاهی وضعیتی ذخیره‌سازی شود. از طرفی هر زیرسامانه در سامانهٔ آگاهی وضعیتی، دانشی را تولید می‌کند. این داده‌ها نیز توسط مولد صحنهٔ نبرد سایبری به شکل استانداری تبدیل شده و در مخزن دانش نگهداری می‌شود.

مدل‌سازی صحنهٔ نبرد سایبری

ورودی‌های اصلی مدل، شامل هشدارهای همبسته‌شدهٔ حسگرها، اطلاعات اجزای محیط (میزبان، سرویس، مسیریاب، دیوارآتش و کاربران) و اطلاعات آسیب‌پذیری‌ها است. موتور صحنهٔ نبرد سایبری با تجمیع و یکپارچه‌سازی مدل شبکه، مدل آسیب‌پذیری، مدل سرویس و مسیر

حمله در محور زمان مدل صحنهٔ نبرد سایبری را در یک ساختار درختی تولید می‌کند. در این ساختار امکان مشاهدهٔ اجزای استفاده‌شده در صحنه و همچنین ویژگی‌های آنها وجود دارد. هر گره مانند ایستگاه کاری ویژگی‌هایی مرتبط با سناریوهای حملهٔ سایبری مانند آدرس IP، فهرست دسترسی، سرویس‌های فعال، سامانهٔ تشخیص/ جلوگیری نفوذ، قابلیت دسترسی به اینترنت، وضعیت در محور زمان، وضعیت فعلی، سیستم‌عامل، ضریب حساسیت و غیره را دارد.

الگوریتم‌های صحنهٔ نبرد سایبری

صحنهٔ نبرد سایبری بستری مناسب به‌منظور انجام تحلیل‌های امنیتی است. در ادامه الگوریتم‌های تحلیلی استفاده شده، تشریح شده است.

محاسبهٔ ضرایب حساسیت

ضریب حساسیت به‌منظور تعیین شدت حساسیت یک عنصر در محیط سایبری است که در ارزیابی اثر و ریسک استفاده می‌شود. ضریب حساسیت برای محدوده، مأموریت، نوع گام حمله از طریق مدیر شبکه و گروه کانونی ایجاد می‌شود. ضریب حساسیت آسیب‌پذیری توسط چارچوب CVSS محاسبه می‌شود. برای هر سرویس حداقل یک مأموریت تعیین می‌شود که هر یک از آنها دارای درجهٔ اهمیت متفاوتی است، برای مثال اهمیت مأموریت سرویس پایگاه داده بالاتر از مأموریت سرویس اشتراک‌گذاری فایل است. مقدار ضرایب حساسیت بین ۰ و ۱ است که حساسیت صفر نشان‌دهندهٔ بی‌ارتباط بودن آن جزء با مأموریت و حساسیت ۱ نشان‌دهندهٔ ضرورت کامل آن جزء برای تحقق مأموریت است.

ارزیابی ریسک

هدف مدیریت ریسک، حفاظت از سازمان برای انجام مأموریت سازمان است که می‌توان آن را به دو بخش اصلی ارزیابی و تقلیل ریسک تقسیم کرد (موسوی و یوسفی، ۱۳۹۴). ارزیابی ریسک یک سرویس در کل شبکه برابر است با مجموع امتیازهای حساسیت آسیب‌پذیری‌های سرویس تقسیم‌بر تعداد آسیب‌پذیری‌ها در عدد ۱۰. طبق رابطه هر چه تعداد آسیب‌پذیری‌ها به همراه ضریب حساسیت آسیب‌پذیری‌ها بیشتر باشد ریسک آن سرویس بیشتر است و برعکس.

ارزیابی اثر حمله‌بر اجزای صحنه

ارزیابی اثر به‌منظور تعیین میزان اثر مخرب هر گام حمله‌بر روی هر یک از اجزای شبکه است. به‌ازای تزریق هر گام حمله به صحنه، ارزیابی اثر روی هر یک از اجزای صحنه (سرویس،

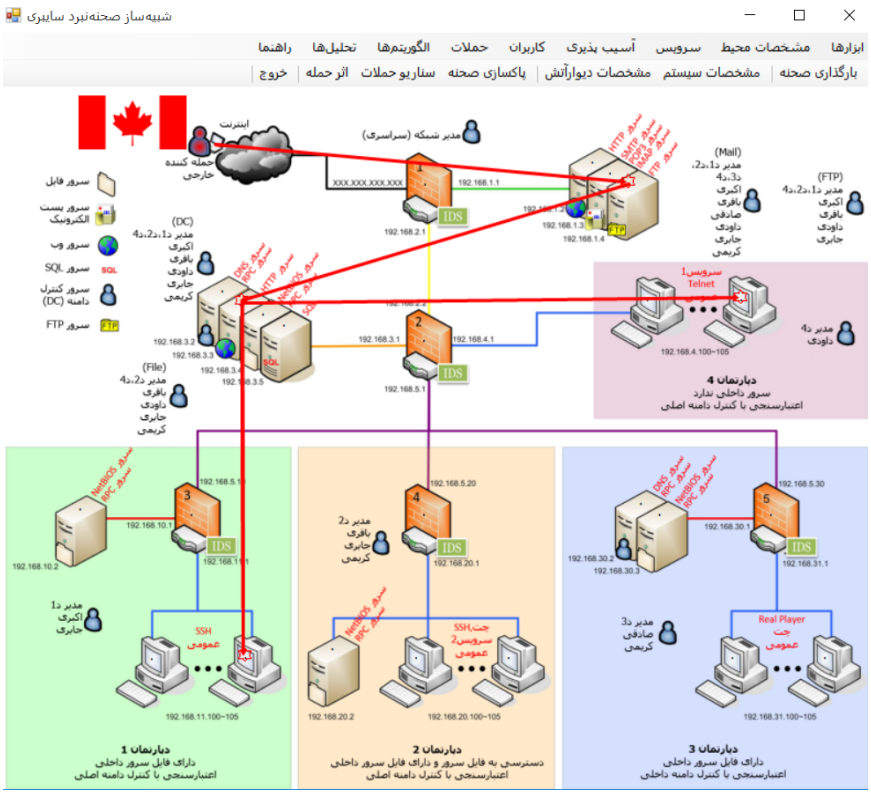
میزبان، کاربر و کل شبکه) انجام می‌شود. ارزیابی اثر کل شبکه بر اساس میزان خسارت نهایی واردشده به کل اجزای شبکه محاسبه می‌شود.

اثر سرویس

اثر سرویس، میزان خسارت واردشده به یک سرویس در اثر اجرای یک گام حمله است. اثر گام حملهٔ m بر سرویس n (رابطهٔ ۱) برابر با حساسیت نوع گام حمله ضرب در حساسیت سرویس n ضرب در ماکزیمم امتیاز حساسیت آسیب‌پذیری‌های استفاده‌شده (مجموعهٔ K) در گام حملهٔ m در زمان t است.

رابطه ۱)

$$\begin{aligned} Impact S_n(AttackStep_m) \\ &= C(\text{AttackStep}) * C(S_n) \\ &* \max_{k \in K(S_n.t)} (cvss(vul_k)); [0.1] \end{aligned}$$



شکل ۲. شبیه‌سازی مدل شبکه (یافتهٔ تحقیق)

اثر میزبان

اثر میزبان، میزان خسارت واردشده به یک میزبان در اثر اجرای یک گام حمله است. اثر گام حملهٔ m بر میزبان n (رابطهٔ ۲) برابر با ضریب حساسیت میزبان n ضرب در ماکزیمم اثر به‌دست‌آمده از گام حملهٔ m بر سرویس‌های میزبان n (مجموعهٔ K) در زمان t است.

رابطهٔ ۲)
$$ImpactH_n(AttackStep_m) = C(H_n) * \max_{k \in K(H_n.t)}(ImpactS_k) ; [0.1]$$

اثر کاربر

هر کاربر از میزبان‌های مختلفی استفاده می‌کند. اثر کاربر، میزان خسارت واردشده به هر کاربر در اثر اجرای یک گام حمله است، در نتیجه به‌ازای هر گام حمله تعدادی از کاربران تحت تأثیر قرار خواهند گرفت. اثر گام حملهٔ m بر کاربر n (رابطهٔ ۳) برابر با ضریب حساسیت نوع کاربر n ضرب در ماکزیمم اثر میزبان به‌دست‌آمده از گام حملهٔ m بر میزبان‌های کاربر n (مجموعهٔ K) در زمان t است.

رابطهٔ ۳)
$$ImpactU_n(AttackStep_m) = C(U_n) * \max_{k \in K(U_n.t)}(ImpactH_k) ; [0.1]$$

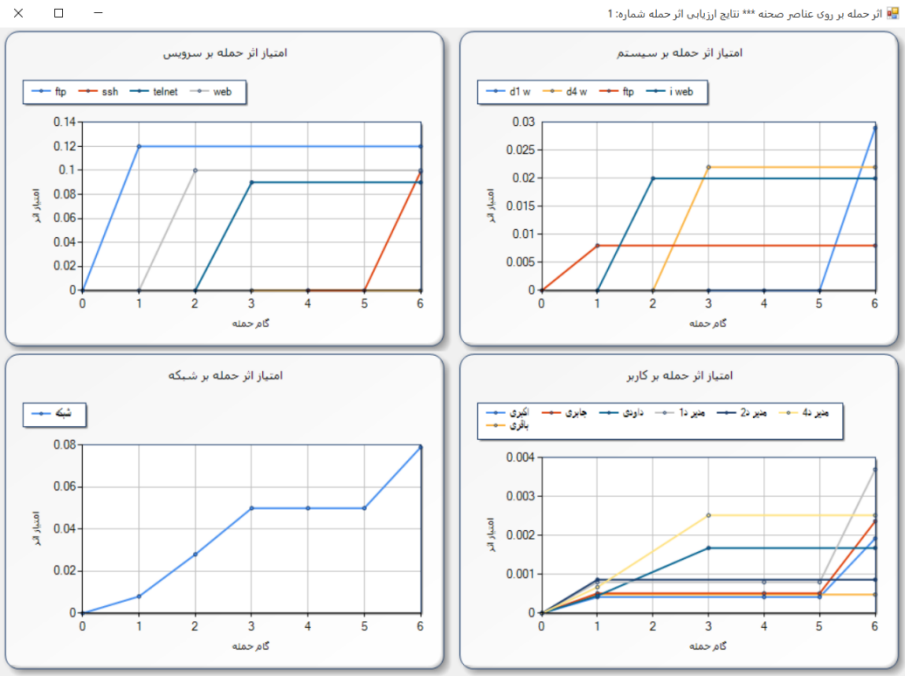
اثر کل شبکه

اثر کل شبکه، میزان خسارت واردشده به کل شبکه در اثر اجرای یک گام حمله است. اثر گام حملهٔ m بر کل شبکه برابر با مجموع اثر میزبان‌های قربانی تا گام حملهٔ m است. با توجه به اینکه این امتیاز از تجمیع امتیاز میزبان (همچنین امتیاز سرویس‌ها و آسیب‌پذیری‌های شبکه) به‌دست می‌آید، در نتیجه امکان نظارت بر کل شبکه را به تحلیلگران امنیتی و مدیر شبکه می‌دهد.

امتیازهای اثر مرجع

به‌منظور داشتن مبنای مقایسه و محاسبهٔ میزان خسارت به امتیاز مرجع برای هر امتیاز اثر نیاز داریم. امتیاز مرجع بالاترین امتیاز اثری است که آن جزء می‌تواند داشته باشد. به‌طور مثال امتیاز مرجع یک میزبان به‌معنای سوءاستفاده از تمام آسیب‌پذیری‌های مربوط به سرویس‌های آن

میزبان با بالاترین امتیاز خسارت است. امتیاز مرجع یک کاربر بیشترین امتیاز اثر بالقوهٔ ناشی از هک شدن کلیهٔ میزبان‌های مربوط به آن کاربر را نشان می‌دهد.



شکل ۳. نمودارهای مربوط به نتیجهٔ الگوریتم‌های ارزیابی اثر (یافتهٔ تحقیق)

تزریق حمله

سناریوی حملهٔ نمونه برای تزریق به شبیه‌ساز دارای ۶ گام و با هدف حملهٔ نفوذ به فایل سرور خارجی، وب سرور داخلی، خوشهٔ دپارتمان ۴ و در انتها خوشهٔ دپارتمان ۱ است. نوع حملهٔ خارجی با مبدأ اینترنت و استفاده از آسیب‌پذیری‌های منع سرویس است. بعد از تزریق حمله به صحنه نتیجهٔ ردگیری آن در شکل ۲ و نتایج ارزیابی اثر در شکل ۳ ارائه شده است. با توجه به پایگاه دادهٔ آدرس‌های اینترنتی صحنه، مبدأ حمله شهر اوتاوا در کانادا و بیشترین خسارت به ایستگاه کاری دپارتمان ۱، مدیر دپارتمان ۱ و سرور وب داخلی وارد شده است. امتیاز اثر شبکه نشان‌دهندهٔ اثر حمله به کل شبکه است. فرض شده گام‌های حمله به‌صورت پشت هم و بدون وقفهٔ زمانی اجرا می‌شوند.

همان‌طور که بیان شد یکی از مسائل، عدم وجود ابزاری برای ارائهٔ راهکارهای امنیتی با قابلیت اولویت‌بندی در راستای ارتقای سطح امنیت کل شبکه است. انتخاب یک معماری امنیتی بهینه که ترجیحاً با کمترین تغییرات و حداقل هزینه بتوان به سطح مطلوبی از امنیت دست پیدا کند، از مسائل مدیران شبکه‌ها است که این امکان در صحنهٔ نبرد پیشنهادی فراهم شده است. به‌طور مثال در شبکهٔ نمونه پس از تحلیل‌ها مشخص شد بیشترین نفوذهای صورت‌گرفته به دلیل سوءاستفاده از آسیب‌پذیری‌های سرویس FTP ویندوز است که با ارتقای این سرویس و سیستم عامل آن سطح امنیت شبکه تا حد زیادی ارتقا پیدا خواهد کرد.

نتیجه‌گیری و پیشنهادها

یکی از مهم‌ترین مؤلفه‌های فرماندهی و کنترل سایبری آگاهی وضعیتی سایبری است. به‌منظور دستیابی به آگاهی وضعیتی سایبری، به پایش دقیق و اجرای مانورهای سایبری نیاز داریم. موتور صحنهٔ نبرد با ایجاد مخزن دانش آگاهی وضعیتی، اطلاعات لازم برای تحلیل‌های امنیتی را فراهم می‌کند که شامل مشخصات به‌روز آسیب‌پذیری‌ها، سناریوی حملات، مدل سرویس، مدل شبکه و مدل صحنهٔ نبرد سایبری است. پویاسازی، ردگیری، انطباق حملات، تحلیل‌های آماری و واسط اطلاعاتی آگاهی وضعیتی از وظایف موتور صحنهٔ نبرد است. الگوریتم‌های ارائه‌شده در زیرسامانهٔ ارزیابی اثر و ریسک، آسیب‌پذیری‌ها و تهدیدهای بالقوهٔ محیط سایبری را شناسایی و رتبه‌بندی می‌کند و با تزریق حملات سایبری ردیابی و تحلیل اثر حمله‌بر شبکه انجام می‌شود. نمایش گرافیکی توپولوژی، وضعیت اجزای شبکه، رد حمله، تحلیل‌های آماری، واسط کاربری مدیریت صحنه، ارزیابی اثر و ریسک توسط زیرسامانه مصورسازی انجام می‌شود. همان‌طور که در بخش یافته‌های پژوهش مشاهده شد، امکان اجرای مانورهای سایبری و شناسایی تهدیدها و آسیب‌پذیری‌های شبکه در این شبیه‌ساز به وجود آمده است. گروه‌های کانونی به‌عنوان روش پژوهش کیفی به‌منظور ارزیابی مدل‌سازی انتخاب شده است. به‌منظور بررسی ارزیابی و بررسی عملکرد مدل شبکهٔ ملی از سامانهٔ کارت هوشمند سوخت استفاده شده است. هدف نهایی ارائهٔ ابزار دفاع سایبری مبتنی بر آگاهی وضعیتی است، به‌گونه‌ای که به تصمیم‌گیری درست و به‌موقع برای مقابله با حملات سایبری منجر شود.

به‌منظور انجام کارهای آتی، پیاده‌سازی شبیه‌سازی صحنهٔ نبرد با استفاده از روش ABM (agent base modelling) پیشنهاد می‌شود. در این روش اجزای صحنه مانند میزبان‌ها، حمله‌کننده، دیوارآتش، حسگرهای امنیتی و سرویس‌ها به‌عنوان عوامل در نظر گرفته می‌شوند.

فهرست منابع

حاج ملک، م.، توکلی، ا. (۱۳۹۵). ارزیابی سطح امنیت در تجارت الکترونیک با استفاده از آنتروپی شانون و تئوری دمپسترشافر. *مدیریت فناوری اطلاعات*، ۷(۱)، ۱۰۰-۷۷.

ونکی، م.، تقوا، م.، تقوی فرد، س.، فیضی، ک. (۱۳۹۶). مدل پیاده‌سازی مدیریت امنیت فناوری اطلاعات در صنعت بانکداری ایران. *مدیریت فناوری اطلاعات*، ۹(۲)، ۴۰۴- ۳۷۹.

عرب‌سرخی میشابی، ا.، موسی خانی، م. و مانیان، ا. (۱۳۹۵). ارائهٔ مدلی مرجع برای تبیین الزامات امنیتی در حوزهٔ یادگیری الکترونیکی از نگاه ذی‌نفعان مختلف. *مدیریت فناوری اطلاعات*، ۸(۱)، ۱۵۴- ۱۴۱.

موسوی، پ.، یوسفی زنوز، ی. و حسن‌پور، ا. (۱۳۹۴). شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانکداری. *مدیریت فناوری اطلاعات*، ۷(۱)، ۱۸۴-۱۶۳.

اسفندیارپور، ر. و اکبری، م. (۱۳۹۵). شناسایی الگوهای ذهنی کارمندان در خصوص سیاست‌های امنیت اطلاعات. *مدیریت فناوری اطلاعات*، ۸(۲)، ۲۳۰- ۲۱۵.

بازرگان، ع. (۱۳۹۵). *مقدمه‌ای بر روش‌های تحقیق کیفی و آمیخته: رویکردهای متداول در علوم رفتاری* (چاپ سوم). تهران، نشر دیدار.

لطفیان، س. (۱۳۷۶)، *استراتژی و روش‌های برنامه‌ریزی استراتژیک*، تهران، وزارت امور خارجه ـ علوم سیاسی.

Ashtiani, M. & Abdollahi Azgomi M. (2014). A Distributed Simulation Framework for Modeling Cyber Attacks and the Evaluation of Security Measures. *Simulation: Transactions of the Society for Modeling and Simulation International*, 90(9), 1071-1102.

Bazargan, A. (2010). *An introduction to the qualitative and mixed methods research approaches used in behavioral science*. Didar publication, Tehran. (*in Persian*)

Endsley, Mica R. (1995). Toward a theory of situation awareness in dynamic systems. *Human Factors Journal,* 37(1), 32–64.

Esfandiarpour, R. & Akbari, M. (2016). Identify employee mindset patterns about information security policies. *Journal of Information Technology Management*, 8(2), 215-230. (*in Persian*)

Habibi, A., Alizadeh, K. & Meshkini, H. (2013). Using fuzzy logic and GIS tools for seismic vulnerability of old fabric in Iranian cities (Case study: Zanjan city), *Journal of Intelligent & Fuzzy Systems,* 25(4), 965-975.

Holsopple, J., Sudit, M. & Yang, S. (2015). *Cyber Defense and Situational Awareness.* in Springer, USA.

Haj Malek, M. & Tavakoli, A. (2016). Evaluating the level of security in e-commerce using Shannon entropy and Shafer's Dempester theory. *Journal of Information Technology Management*, 8(1), 77-100. (*in Persian*)

Kotenko, I. & Chechulin, A. (2013, June). A cyber attack modeling and impact assessment framework. *In Cyber Conflict (CyCon), 2013 5th International Conference on (pp. 1-24)*. IEEE.

Lippmann, R. P. & Ingols, K. W. (2005). *An annotated review of past papers on attack graphs* (No. PR-IA-1). Massachusetts inst of tech lexington lincoln lab.

Lotfian, S. (1997). *Strategy & Strategic Planning*. Ministry of Foreign Affairs, political science. (*in Persian*)

Moskal, S., Wheeler, B., Kreider, D., Kuhl, M. E. & Yang, S. J. (2014, October). Context model fusion for multistage network attack simulation. *InMilitary Communications Conference* (MILCOM), 2014 IEEE (pp. 158-163). IEEE.

Mousavi, P., Yousefi Zenuz, R. & Hasanpour, A. (2015). Identifying Information Security Risks Using the Fuzzy Delphi Method in the Banking Industry. *Journal of Information Technology Management*, 7(1), 163-184. (*in Persian*)

Nguyen, P. H., Ali, S. & Yue, T. (2016). Model-based security engineering for cyber-physical systems: A systematic mapping study. *Information and Software Technology*, 83, 116-135.

Phillips, C. & Swiler, L. P. A. (1998). graph-based system for network vulnerability analysis system. *in In Proceedings of the 1998 workshop for new security paradigms*, New York.

Arab Sorkhi Mishabi, A., Mousa Khani, M. & Manian, A. (2016). Provides a reference model for security requirements in the field of e-learning from the perspective of different stakeholders. *Journal of Information Technology Management*, 8(1), 141-154. (*in Persian*)

Schneier, B. (1999). Attack trees. *Dr. Dobb's journal*, 24(12), 21-29.

Shakibazad, M. & Rashidi, A. (2017). A framework to achieve dynamic model of cyber battlefield. *in Bulletin de la Société Royale des Sciences de Liège*, 86, 474 – 483.

T. N. S. Inc. (2017). *The Nessus Vulnerability Network Scanner*. Available in: http://www.tenable.com/products/nessus-vulnerability-scanner. [Online]

United States Air Force. (2012). *United States Air Force Cyber Vision 2025*. United States Air Force, Washington.

Vanaki, M., Taghva, M., Taghavi Fard, S. & Feizi, K. (2017). IT Security Management Implementation Model in Iranian Bank Industry. *Journal of Information Technology Management*, 9(2), 379-404. (*in Persian*)

Vidalis, S. & Jones, A. (2003). Using vulnerability trees for decision making in threat assessment. *in ECIW Proceedings of the 2nd European Conference on Information Warfare and Security*, UK, p. 329.

Wheeler, B. F. (2014). *A Computer Network Model for the Evaluation of Moving Target Network Defense Mechanisms*. Thesis, Rochester Institute of Technology.

Yang, S. J., Holsopple, J. & Liu, D. (2009, May). Elements of impact assessment: a case study with cyber attacks. *In SPIE Defense, Security, and Sensing (pp. 73520D-73520D). International Society for Optics and Photonics.*