

A Computational Method Based on CVSS For Quantifying the Vulnerabilities in Computer Networks

Mohammad Hossein Sherkat¹ | Shahriyar Mohammadi² | Mona JamiPour³

1. PhD in Systems Management; Management School; University of Tehran; Iran
mh_sherkat@yahoo.com
2. [Corresponding Author] Assistant professor; Department of Industrial engineering; Khajeh Nasir Toosi University of Technology (KNTU); Tehran, Iran
mohammadi@kntu.ac.ir
3. PhD in Systems Management; Management School; University of Tehran; Iran
mjamporazmay@yahoo.com

Iranian Journal of
**Information
Processing &
Management**

Abstract: Network vulnerability taxonomy has become increasingly important in the area of information and data exchange not only for its potential use in identification of vulnerabilities but also in their assessment and prioritization. Computer networks play an important role in information and communication infrastructure. However, they are constantly exposed to a variety of vulnerability risks. In their attempts to create secure information exchange systems, scientists have concentrated on understanding the nature and typology of these vulnerabilities. Their efforts aimed at establishing secure networks have led to the development of a variety of methods and techniques for quantifying vulnerability.

The objective of the present paper is developing a method based on the second edition of common vulnerability scoring system (CVSS) for the quantification of Computer Network vulnerabilities. It is expected that the proposed model will help the identification and effective management of vulnerabilities by their quantification.

Keywords: Vulnerability; Computer Network Vulnerability; Taxonomy of Vulnerabilities; ITU-TX-805 Security Architecture; Quantifying Vulnerabilities; Common Vulnerability Scoring System

Iranian Research Institute
for Information Science and Technology
(IranDoc)

ISSN 2251-8223

eISSN 2251-8231

Indexed by SCOPUS, ISC, & LISTA

Vol. 29 | No. 4 | pp. 1107-1145

Summer 2014

<https://doi.org/10.35050/IJPM010.2014.020>



ارائه یک روش محاسباتی به منظور کمی سازی میزان آسیب پذیری شبکه های رایانه ای بر اساس سیستم امتیازدهی آسیب پذیری متعارف

محمدحسین شرکت^۱ | شهریار محمدی^۲ | مونا جامی پور^۳

۱. دکتری مدیریت سیستم ها؛ گروه مدیریت فناوری اطلاعات؛ دانشگاه تهران؛ دانشکده مدیریت
mh_sherkat@yahoo.com
۲. [پدیدآور رابط] دکتری فناوری اطلاعات؛ استادیار؛ گروه فناوری اطلاعات؛ گروه مهندسی
صنایع؛ دانشگاه خواجه نصیرالدین طوسی
mohammadi@kntu.ac.ir
۳. دکتری مدیریت سیستم ها؛ گروه مدیریت فناوری اطلاعات؛ دانشکده مدیریت؛ دانشگاه تهران
mjamporzmay@yahoo.com

مقاله پژوهشی

دریافت: ۱۳۹۱/۰۶/۱۴
پذیرش: ۱۳۹۲/۱۲/۱۸

دانشگاه مدیریت اطلاعات

فصلنامه | علمی پژوهشی
پژوهشگاه علوم و فناوری اطلاعات ایران
(ایرانداک)

شاپا (چاپی) ۸۲۲۳-۲۴۰۱
شاپا (الکترونیکی) ۸۲۳۱-۲۴۰۱
نمابه در JLISTA، ISC، و SCOPUS
ijpm.irandoc.ac.ir

دوره ۲۹ | شماره ۴ | صص ۱۱۰۷-۱۱۴۵
تابستان ۱۳۹۳

<https://doi.org/10.35050/IJPM010.2014.020>

چکیده: افزایش تعداد آسیب پذیری ها و پیچیدگی آنها در حوزه تبادل داده و اطلاعات، اهمیت مسئله کمی سازی آسیب پذیری ها را هم به جهت تعیین میزان آن و هم از نظر اولویت دهی و مدیریت منابع، بیش از پیش حائز اهمیت ساخته است. شبکه های رایانه ای به دلیل داشتن جایگاه پُراهمیت در زیرساخت ارتباطی و تبادل داده ها و اطلاعات همواره در معرض آسیب پذیری های متعددی قرار داشته اند و این مسئله لزوم محاسبه کمی میزان آسیب پذیری ها را به منظور امکان دستیابی به شبکه هایی امن، بیش از پیش معطوف نظر محققان ساخته است. در این مقاله تلاش شده به منظور محاسبه کمی آسیب پذیری های شبکه، یک روش توسعه یافته بر پایه معماری امنیت ITU-TX-805 و بر پایه ویرایش دوم سیستم امتیازدهی آسیب پذیری متعارف (CVSS) پیشنهاد گردد. هدف روش پیشنهادی در این تحقیق، فراهم آوردن یک ساختار کمی سازی به منظور امکان شناسایی میزان آسیب پذیری ها و مدیریت مؤثر آنها می باشد.

کلیدواژه ها: آسیب پذیری؛ آسیب پذیری شبکه های رایانه ای؛ معماری امنیت ITU-TX-805؛ کمی سازی آسیب پذیری ها؛ سیستم امتیازدهی آسیب پذیری متعارف (CVSS)



۱. مقدمه

میزان اطلاعات مهم، حساس و حیاتی شرکت‌ها و سازمان‌های دولتی و غیردولتی بر روی پایگاه‌های اطلاعاتی که از طریق شبکه‌های محلی و یا جهانی در سراسر دنیا به یکدیگر متصل شده‌اند تا در هر لحظه امکان استفاده از این اطلاعات فراهم باشد، روزبه‌روز در حال افزایش است. این در حالی است که شبکه‌های رایانه‌ای نیز همانند سایر سیستم‌های رایانه‌ای به‌طور کامل امن نبوده و دارای نقاط ضعف و آسیب‌پذیر بسیاری می‌باشند و امکان رخنه و نفوذ به درون آنها و در نتیجه سرقت اطلاعات و یا فروپاشی آنها وجود دارد و همین مسئله موجب گردیده شبکه‌های رایانه‌ای در معرض آسیب‌پذیری‌های متعددی قرار داشته باشند (امیدیان و دیگران ۱۳۸۸).

آسیب‌پذیری بستری بالقوه و مستعد برای وقوع حمله است که هر زمان اتفاق بیفتد، می‌تواند رفتاری نامطلوب و غیرصحیح به وجود آورد (Hansmann et al 2005). بر اساس تعریف «راما کریشان» و «سکار» آسیب‌پذیری یکی از نقاط ضعف سیستم است که از آن می‌توان برای به‌خطر انداختن امنیت سیستم سوءاستفاده کرد (Ramakrishnan and Sekar 1998). «بیشاپ» آسیب‌پذیری را به‌عنوان یکی از ویژگی‌های سیستم می‌داند که از یک سو به‌طور بالقوه باعث سوءاستفاده از سیستم می‌شود و از سوی دیگر می‌تواند خود نتیجه یک یا چند حمله یا سوءاستفاده دیگر باشد (Bishop 1995). «آمان» و همکاران آسیب‌پذیری را عبارت از هر ویژگی سیستم رایانه‌ای تعریف می‌کند که امکان نقض خط‌مشی‌های امنیتی آن سیستم را به فرد یا افرادی بدهد (Ammann 2002). در تعریف دیگری از بیشاپ آسیب‌پذیری به معنای وجود ضعف امنیتی در سیستم تعریف شده که امکان سوءاستفاده از سیستم و تهدید صحت و جامعیت اطلاعات را از جانب مهاجمان فراهم می‌آورد (Bishop 2003).

ارزیابی درجه آسیب‌پذیری برای هر یک از ابعاد آسیب‌پذیر در شبکه‌های رایانه‌ای از اهمیت بالایی برخوردار است، چرا که هر چه یک بُعد در یک سیستم شبکه آسیب‌پذیرتر باشد، آن بُعد بیشتر مورد سوءاستفاده مهاجمان قرار می‌گیرد. از سوی دیگر، برای ایمن‌سازی و دستیابی به شبکه‌هایی امن، شناخت میزان آسیب‌پذیری به‌منظور امکان مدیریت مؤثر منابع در مواجهه با آسیب‌ها امری لازم و اساسی است.

در این مقاله تلاش شده که بر پایه جنبه‌های امنیتی معماری امنیت ITU-TX-805

نسبت به ارائه یک روش کمی سازی در حوزه محاسبه آسیب پذیری های شبکه های رایانه ای بر پایه ویرایش دوم سیستم امتیازدهی آسیب پذیری متعارف^۱ با عنوان NCVSS اقدام گردد. معماری امنیت ITU-TX-805 در مقایسه با سایر چارچوب ها و معماری های امنیتی جامع تر بوده و ضمن قابلیت به کارگیری برای کلیه شبکه ها، یک نمای جامع و بالا به پایین از امنیت شبکه را برای اجزاء، سرویس ها و کاربردهای شبکه جهت شناسایی، پیشگیری و اصلاح آسیب پذیری ها فراهم می نماید (حاجیان و دیگران ۱۳۸۸).

این مقاله در ۵ بخش تنظیم شده است. پس از مقدمه، در بخش دوم به مطالعه ادبیات موضوع و طبقه بندی آسیب پذیری ها پرداخته می شود. در بخش سوم، روش پیشنهادی برای محاسبه کمی آسیب پذیری ها ارائه شده و بخش چهارم به آزمون روش پیشنهادی می پردازد. بخش پنجم شامل جمع بندی نتایج و نتیجه گیری است.

۲. مروری بر ادبیات موضوع

در مطالعه علمی هر حوزه جدید علمی وجود ساختار و یا چارچوب بررسی به عنوان پیش نیازی لازم و مهم برای مطالعه ساختارمند آن و ایجاد یک زبان مشترک در آن حوزه امری حیاتی است (Howard 1998). «کرسول» با بیان اهمیت وجود چارچوبی برای بررسی در مدیریت مؤثر مطالعات حوزه آسیب پذیری معتقد است که تعریف چارچوب مؤثر می تواند زمینه ساز تعریف یک دسته بندی مناسب به منظور طبقه بندی آسیب پذیری ها گردیده و این طبقه بندی خود مبنایی برای مدیریت مؤثر آسیب پذیرها گردد (Krsul 1998). «لاف» ضمن بیان ضرورت ساخت یافته بودن، جامعیت، وضوح و کارآمدی در هر نوع ساختار مدیریت آسیب پذیرها، معتقد است که یک ساختار با فراهم کردن مفاهیم مشترک در دسته بندی آسیب پذیری ها، راه ساخت یافته ای را جهت مشاهده، تحلیل و ارزیابی کمی و کیفی آسیب پذیری ها فراهم می نماید (Lough 2001).

«بیشاپ» معتقد است که اولین مرحله برای مدیریت مؤثر آسیب پذیری ها، فهم آسیب پذیری ها بر اساس دسته بندی آنها بر مبنای مشخصاتشان در رده بندی است، چرا که این کار تعداد زیادی از آسیب پذیری ها را بر طبق یک گروه بندی، قابل فهم می سازد (Bishop 2003). بنا به اعتقاد «بیشپی» و «هالینگورث» یکی از اهداف تولید رده بندی های

1. Common Vulnerability Scoring System: CVSS

آسیب پذیری، توسعه ابزارهای خودکار جهت انجام ارزیابی های کمی در حوزه امنیت است (Bisbey & Hollingworth 1978).

تاکنون رده بندی های متعددی در حوزه آسیب پذیری ارائه شده است. جدول شماره ۱ خلاصه مهم ترین رده بندی های انجام شده در حوزه آسیب پذیری و مشخصات کلیدی هر یک را نمایش می دهد. شاید بتوان گفت که اولین دسته بندی در حوزه آسیب پذیری در سال ۱۹۶۷ در آمریکا انجام پذیرفته است. در این تحقیق دولت فدرال مراکز محاسباتی را وادار به مطالعه و بررسی مسائل و امور مرتبط با آسیب پذیری های نرم افزاری، به خصوص سیستم های عامل نمود (Ammala 2004).

جدول ۱. خلاصه مهم ترین رده بندی های انجام شده در حوزه آسیب پذیری

ردیف	محقق / محققان	مبنای رده بندی	تمرکز موضوعی	مشخصه
۱	Abbott et al, 1976	اشکالات و آسیب پذیری های زمان برنامه نویسی و تولید کد برنامه	سیستم عامل ها	تک لایه
۲	Bisbey et al, 1978	خطاهای حفاظتی در فرایند استفاده	سیستم عامل ها	تک لایه
۳	Ristenbatt, 1988	طراحی شبکه و ویژگی های در معرض آسیب	شبکه ها	تک لایه
۴	Landwehr et al, 1994	پیدایش، مکان رخنه و زمان ایجاد رخنه	نرم افزارها	تک لایه
۵	Aslam, 1995	اشکالات و آسیب پذیری های زمان برنامه نویسی و تولید کد برنامه	سیستم عامل UNIX	تک لایه
۶	Bishop, 1995	اشکالات و آسیب پذیری های زمان برنامه نویسی و تولید کد برنامه	نرم افزارها	تک لایه

ردیف	محقق / محققان	مبنای رده بندی	تمرکز موضوعی	مشخصه
۷	Du, 1997	انواع حملات و آسیب پذیری های دیواره های آتش	شبکه ها	تک لایه
۸	Bishop, 1999	طبیعت، زمان رخداد، سوء استفاده، اثر، حداقل تعداد اجزاء آسیب پذیر، منبع شناسایی	عمومی	تک لایه
۹	Kamara, 2003	انواع حملات و آسیب پذیری های دیواره های آتش	دیواره های آتش	تک لایه
۱۰	Pothamsetty et al, 2004	رخنه های موجود در پروتکل های نرم افزاری	پروتکل	تک لایه
۱۱	Weber, et al, 2005	چگونگی پیدایش و علل ایجاد رخنه	نرم افزارها	تک لایه
۱۲	Hamed et al, 2006	ناسازگاری سیاست امنیتی	شبکه ها	تک لایه
۱۳	Asosheh et al, 2008	خطرات ناشی از انکار سرویس توزیع شده (DDoS)	شبکه ها	تک لایه
۱۴	Wiesauer et al, 2009	الگوی حملات	نرم افزارها	تک لایه
۱۵	Ryoo et al, 2009	چگونگی پیدایش و علل ایجاد رخنه	شبکه های بی سیم	سلسله مراتبی و چندبعدی
۱۶	Zeidanloo et al, 2010	IDS و honeynet ها	Botnet ها	تک لایه
۱۷	Alvi and Zulkernine, 2011	رده بندی آسیب پذیری ها بر اساس فازهای دوره عمر نرم افزار	نرم افزار	---

ردیف	محقق / محققان	مبنای رده‌بندی	تمرکز موضوعی	مشخصه
۱۸	Tripathi and Singh, 2011	طبقه‌بندی الگوهای آسیب‌پذیری پایگاه داده به‌منظور شناسایی میزان ریسک امنیتی	پایگاه داده	---
۱۹	Ahmad et al., 2011	بهبود روش‌های موجود در طبقه‌بندی آسیب‌پذیری‌های نرم‌افزار از طریق تمرکز روی زبان برنامه‌نویسی C	نرم‌افزار	---
۲۰	Kuhn, 2011	رده‌بندی آسیب‌پذیری‌ها بر اساس سیاست کنترل دسترسی و شناسایی خطاهای پیکره‌بندی	تست کلاس‌های خاص معرفی شده	چندلایه‌ای و چندبعدی
۲۱	Hunt and Slay, 2011	طبقه‌بندی آسیب‌پذیری‌ها به‌منظور دست‌یابی به فناوری‌های جدید برای مقابله با انواع مکانیزم‌های جدید دفاعی	سیستم‌های توسعه یافته مانند محاسبات ابری، بدافزارهای سه‌بعدی و VOIPها	---
۲۲	Yan et al., 2011	دسته‌بندی آسیب‌پذیری‌ها با استفاده از آزمایش‌های تجربی به‌منظور ارزیابی کارایی الگوهای معنایی	نرم‌افزار	---
۲۳	Shijia et al., 2011	۱- تکنیک‌های تست آسیب‌پذیری Brute Force، ۲- تست آسیب‌پذیری داده با تغییر پروتکل پیام‌ها	سرورها و پروتکل شروع جلسه	---
۲۴	Szidarovszky and Yi, 2011	استفاده از الگوریتمی با متغیرهای تصمیم‌گیری ساده به‌منظور تشخیص مکان‌یابی منابع به‌صورت امن	شبکه	---

ردیف	محقق / محققان	مبنای رده بندی	تمرکز موضوعی	مشخصه
۲۵	Gallon and Bascou, 2011	۱- استفاده از چارچوب CVSS به منظور نمره دهی عددی به آسیب پذیری های ثبت شده در پایگاه های داده CVE، ۲- ایجاد ارتباط بین گراف های حمله با چارچوب CVSS به منظور ارزیابی اثر حمله ها بر میزبان شبکه هدف	شبکه های رایانه ای	---
۲۶	Vijayakumar and Muthuchelvi, 2011	استفاده از XDOS و TCP/IP برای کشف اتوماتیک آسیب پذیری های Zombie	نرم افزار	---
۲۷	Shahriar and Zulkernine, 2011	۱- طبقه بندی آسیب پذیری ها با توجه به ویژگی های عمومی در حملات آنلاین ۲- طبقه بندی آسیب پذیری ها بر اساس تفاوت ویژگی های برنامه در حال اجرا با ویژگی های ثبت شده	برنامه های نرم افزاری	---
۲۸	Perla et al., 2011	طبقه بندی آسیب پذیری ها بر اساس خطاهای منطقی، شرایط رقابتی و نتایج عملیات منطقی	سیستم عامل	---
۲۹	Holm et al., 2012	استفاده از چارچوب CVSS به منظور تعیین سطح آسیب پذیری سیستم ها	شبکه های کامپیوتری	---
۳۰	Zhongwen and Yingchun, 2012	رده بندی آسیب پذیری ها بر پایه پنج ویژگی امنیت اطلاعات شامل یکپارچگی، دسترس پذیری، محرمانگی، قابلیت کنترل و قابلیت اعتماد	امنیت اطلاعات	----

ردیف	محقق / محققان	مبنای رده‌بندی	تمرکز موضوعی	مشخصه
۳۱	Xiaohui et al., 2012	طبقه‌بندی آسیب‌پذیری‌های نرم‌افزار از طریق تحلیل فرایند چرخه عمر نرم‌افزار	سیستم‌های توزیع شده در مقیاس وسیع	چند لایه‌ای و چند بعدی
۳۲	Hudic et al., 2012	استفاده از مکانیزم‌های تست نفوذ به منظور طبقه‌بندی آسیب‌پذیری‌های پایگاه داده، سیستم‌های رایانه‌ای و شبکه‌ها	سیستم‌های رایانه‌ای و شبکه‌ها	---
۳۳	JunGang et al., 2012	تشخیص هویت میزبان‌ها به منظور کاهش ریسک‌های آسیب‌پذیری	شبکه‌های رایانه‌ای	سلسله‌مراتبی
۳۴	Maatta and Raty, 2012	استفاده از اسناد XML برای بررسی فعالیت‌های شبکه و کشف آسیب‌پذیری‌ها	شبکه‌های رایانه‌ای	---
۳۵	Shiguo et al., 2012	ارائه متدهای تحلیل آسیب‌پذیری در زمینه امنیت شبکه به منظور تشخیص طبقه‌بندی مناسب برای آسیب‌پذیری‌ها	شبکه‌های ad hoc، ماهواره‌ای، امنیت شبکه	---
۳۶	Corcalciuc, 2012	۱- دسته‌بندی آسیب‌پذیری‌ها با استفاده از نمودارهای SwimLane، ۲- تفسیر معنایی برنامه‌های هم‌روند، لایه‌های انتزاعی، درخت سلسله‌مراتبی و ویژگی‌های ارث‌بری شده از لایه‌های پایین به منظور ارائه دسته‌بندی مناسب از آسیب‌پذیری	زمان و مکان	سلسله‌مراتبی
۳۷	Bhattacharya and Ghosh, 2012	دسته‌بندی آسیب‌پذیری‌ها با استفاده از گراف وابستگی به منظور شناسایی حملات و آسیب‌پذیری‌های به وجود آمده	شبکه	---

ردیف	محقق / محققان	مبنای رده بندی	تمرکز موضوعی	مشخصه
۳۸	Njogu et al., 2013	طبقه بندی آسیب پذیری ها با توجه به انواع خطا و سطح دقت در سرورها	سرورهای HTTP & Apache & IIS	---
۳۹	Wang et al., 2013	معرفی معیار جدید امنیتی به نام k-Zero Day Safety، این معیار به جای شمردن تمام آسیب ها، به ارزیابی آسیب هایی می پردازد که ممکن است تخریب زیادی روی امنیت شبکه بگذارند	شبکه های رایانه ای	---
۴۰	Ben-Porat, 2013	استفاده از Closed-Hash برای ارزیابی ساختار داده به منظور تعیین میزان آسیب پذیری	شبکه های رایانه ای	---
۴۱	Marrone et al., 2013	ارائه زبان مدل سازی برای تحلیل آسیب پذیری ها در برنامه های کاربردی به منظور حفاظت از ساختار حیاتی برنامه ها	نرم افزار	---
۴۲	Kakareka, 2013	استفاده از XML برای ارزیابی آسیب پذیری سیستم	سیستم های رایانه ای	---
۴۳	Wang et al., 2013	استفاده از الگوی پیمایش آسیب پذیری سرویس بر پایه معماری SOA در محیط وب سرویس	محیط های وب سرویس	سلسله مراتبی
۴۴	Zhang et al., 2014	استفاده از سیستم امنیتی تا بتوان با تشخیص آسیب پذیری، آن را به همه کلاینت ها ارسال نمود	نرم افزار	---

با مروری بر مطالعات انجام شده و موارد مندرج در جدول شماره ۱ می توان به این نتیجه رسید که در دسته بندی های ارائه شده معیارها و فاکتورهای متفاوتی برای دسته بندی و رده بندی آسیب پذیری ها استفاده شده است. این معیارها عبارتند از:

- ◇ دسته بندی آسیب پذیری ها با توجه به روشی که از آنها سوء استفاده می شود؛
- ◇ دسته بندی به مؤلفه های نرم افزاری و سخت افزاری و رابطه ای که باعث بروز آسیب پذیری می شو؛
- ◇ دسته بندی بر اساس ماهیت آسیب پذیری و دلایل ایجاد آن؛
- ◇ دسته بندی آسیب پذیری ها بر اساس زمان وقوع آنها؛ و
- ◇ دسته بندی آسیب پذیری ها بر اساس دامنه آن.

با توجه به اینکه در موضوع امنیت شبکه هدف از بررسی و تحلیل آسیب پذیری ها، شناسایی و کشف حمله قبل از وقوع آن بر اساس میزان آسیب پذیری هر یک از مؤلفه های امنیتی به منظور اتخاذ تدابیر لازم در جهت مواجهه با آسیب پذیری است، آنها باید به گونه ای بررسی و رده بندی شوند که امکان محاسبه میزان آسیب پذیری ها را با هدف امکان تعیین نقش و اثر آسیب پذیری های شبکه فراهم آورند (امیدیان و دیگران ۱۳۸۸). بر این اساس یکی از نواقص قابل مشاهده در فعالیت های انجام شده قبلی فقدان یک ساختار کمی سازی در چارچوب های بررسی و طبقه بندی آسیب پذیری هاست.

تاکنون مطالعات محدودی به منظور ارائه روش های ارزیابی و محاسبه کمی آسیب پذیری ها انجام گردیده است. «جورج» و «وامانو» چارچوب عملی عمومی را جهت ارزیابی کمی آسیب پذیری سیستم ها ارائه نموده اند (gheorghie and Vamanu 2004). در این چارچوب، میزان آسیب پذیری سیستم به شکل کمی، و به صورت عددی بین ۰ تا ۱۰۰ اندازه گیری می شود. الحزمی و مالائیا معیاری با نام چگالی آسیب پذیری را به عنوان معیاری جهت ارزیابی میزان آسیب پذیری سیستم ها و امکان پیش بینی نرخ کشف آسیب پذیری ها در آینده معرفی نموده اند (Alhazmi and Malaiya 2005). امامی و جعفریان نیز به ارائه چارچوبی برای محاسبه درجه آسیب پذیری سیستم های مدیریت پایگاه داده های متن باز رایج پرداخته اند (۲۰۰۹). در این مطالعه، روشی برای ارزیابی میزان آسیب پذیری سیستم های هم نوع با استفاده از تعداد آسیب پذیری ها، تعداد نسخ رایج و میزان محبوبیت آنها معرفی شده و چارچوب پیشنهادی برای محاسبه کمی آسیب پذیری

پایگاه های داده متن باز، MySQL، PostgreSQL، Ingres، Firebird مورد استفاده قرار گرفته است (امامی و دیگران ۱۳۸۸). به منظور ایمن سازی و دستیابی به شبکه های امن نیز رویکردهای مختلفی ارائه گردیده که در جدول شماره ۲ به صورت خلاصه به اهم موارد مندرج در تحقیقات سال های اخیر پرداخته شده است.

جدول ۲. رویکردهای متأخر در ایمن سازی و دستیابی به شبکه های امن

سال - محقق	بررسی صورت گرفته	تمرکز موضوعی
(Taheri et al. 2010)	مسیریابی MultiPath برای تشخیص و محافظت از حملات کرم ها	شبکه های بی سیم و موردی
(Nehinbe 2011)	مرور راهنمایی های موجود برای افزایش نظارت بر نفوذ به سیستم	سیستم های رایانه ای
(Yonglin et al. 2011)	ایجاد گراف حمله به منظور تشخیص حملات غیر مستقیم	شبکه های رایانه ای
(Asman et al. 2011)	شبیه سازی عامل گرا با توجه به جریان بسته ها و بررسی رفتار آنها به منظور شناسایی جریان های مخرب	سیستم های رایانه ای، مسیریاب ها و سرورها
(Hudic et al. 2012)	طبقه بندی مناسب برای پوشش فرایند Penetration Test	پایگاه داده، سیستم های رایانه ای
(Kundu et al. 2012)	استفاده از گراف به منظور تحلیل آسیب های امنیتی موجود و تشخیص میزان امن بودن سیستم	شبکه های رایانه ای
(Junshun et al. 2012)	تشخیص خطاها و محل رویداد آنها با استفاده از ابزار SMT به منظور چک کردن صحت داده ها	شبکه های رایانه ای
(Saxena and Hote) 2013	استفاده از تئوری Rough Set به منظور ترکیب فاکتورهای حمله و تشخیص احتمال وقوع حمله	سیستم های رایانه ای LAN
(Jiang et al. 2013)	استراتژی ارزیابی و آگاهی از حملات به صورت عامل گرا	شبکه های رایانه ای

سال - محقق	بررسی صورت گرفته	تمرکز موضوعی
Hernandez-Ardieta) (et al. 2013	طبقه بندی حمله های صورت گرفته در امضای دیجیتال به صورتی که فاز تولید و تصدیق امضای دیجیتال را پوشش می دهد	امضای دیجیتال
(Corona et al. 2013)	طبقه بندی کلی تکنیک های حمله به منظور داشتن تشخیص نفوذ مناسب	سیستم های رایانه ای
Avramescu et al.) (2013	استفاده از Penetration Test برای تشخیص حملات	شبکه های رایانه ای، برنامه های تحت وب، پایگاه داده SQL

۳. روش پیشنهادی

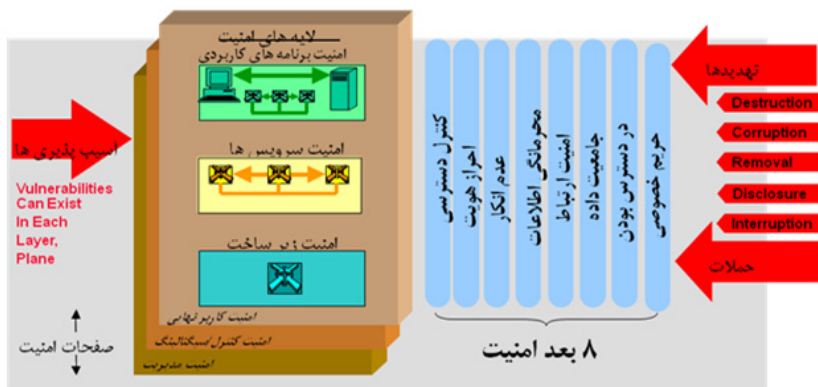
بر اساس آنچه که در بخش قبل اشاره گردید، در این بخش تلاش می شود نسبت به ارائه یک روش محاسباتی به منظور محاسبه کمی میزان آسیب پذیری های شبکه های رایانه ای اقدام گردد. همان گونه که در مقدمه اشاره شد، نخست لازم است ساختار و چارچوب مورد نظر جهت ارائه روش کمی سازی تعریف گردیده و بر اساس آن نسبت به ارائه روش محاسباتی اقدام شود. با توجه به هدف تحقیق، ساختار و چارچوب مورد استفاده باید مشخص نماید که چه فعالیت هایی در ساختار شبکه در معرض آسیب پذیری قرار دارند و باید محافظت شوند تا بر اساس آن بتوان نسبت به محاسبه میزان آسیب پذیری ها اقدام نمود.

برای تعیین این فعالیت ها و تعیین ساختار و چارچوب مربوط در این تحقیق از معماری امنیت ITU-TX-805 استفاده شده است. شکل شماره ۱ نمایی از معماری امنیت ITU-TX-805 را نمایش می دهد. دلایل استفاده از این معماری در روش پیشنهادی را می توان به طور خلاصه چنین بیان کرد:

۱. معماری امنیت ITU-TX-805 به گونه ای طراحی شده که برای کلیه شبکه ها و کاربردها قابل به کارگیری بوده و نگرانی های امنیتی مربوط به مدیریت، کنترل و استفاده از زیرساخت، سرویس ها و کاربردهای شبکه را مد نظر قرار می دهد؛ و

۲. نمای جامع و بالا به پایین از امنیت شبکه را برای عناصر، سرویس ها و کاربردهای شبکه فراهم می کند (مک گی^۱ و دیگران ۲۰۰۴).

ساختار معماری ITU-TX-805 سه مؤلفه ابعاد یا جنبه های امنیتی، لایه های امنیتی، و سطوح امنیتی را شامل است. در این تحقیق به منظور تعیین فعالیت هایی که در معرض آسیب پذیری در ساختار شبکه می باشند، بر روی ابعاد و یا جنبه های امنیتی معماری امنیت اطلاعات تمرکز شده است.



شکل ۱. ساختار معماری امنیت ITU-TX-805 (مک گی و دیگران ۲۰۰۴)

ابعاد امنیتی، مجموعه ای از اقدامات امنیتی است که جهت مشخص کردن جنبه خاصی از امنیت شبکه طراحی شده است. در این معماری، هشت مجموعه مشخص شده در بُعد امنیت شامل کنترل دسترسی، احراز هویت، عدم انکار، محرمانگی داده ها، امنیت ارتباطات، تمامیت داده، قابلیت دسترسی و حریم خصوصی حفاظت در برابر کلیه تهدیدهای امنیتی اصلی فراهم می آید. در این معماری جهت فراهم شدن راه حل امنیت کامل، ابعاد امنیتی را بایستی بتوان برای ساختار سلسله مراتبی تجهیزات و اجزاء شبکه که تحت عنوان لایه های امنیتی نامگذاری می شود، به کار برد. بر این اساس سه لایه امنیتی زیرساخت، سرویس و کاربردی در این معماری تعریف شده است. هر لایه بر روی لایه دیگر ساخته شده تا یک راه حل جامع فراهم شود. در این شرایط لایه زیرساخت، لایه

1. McGee

سرویس و لایه کاربرد را فعال می‌سازد.

معماری امنیت ITU-TX-805 این حقیقت را مشخص می‌کند که هر لایه، آسیب‌پذیری‌های امنیتی متفاوتی دارد. سطوح امنیتی، گروه‌های اصلی فعالیت‌های شبکه هستند که به وسیله ابعاد امنیتی محافظت می‌شوند. در این معماری سه سطح امنیتی برای ارائه سه گروه از فعالیت‌هایی که در شبکه اتفاق می‌افتد، تحت عنوان سطح مدیریت، سطح کنترل و سطح کاربر نهایی تعریف شده است. اعمال بُعد امنیتی بر روی سطوح و لایه‌ها، به ایجاد یک نمای مجتمع منتهی شده و در نهایت ۷۲ نمای امنیتی مجزا شکل می‌گیرد تا بتواند جنبه‌های متفاوت یک رخنه امنیتی یا یک آسیب‌پذیری را موشکافانه ارزیابی نماید.

دلیل تمرکز بر جنبه‌های امنیتی در ساختار مورد استفاده به منظور کمی‌سازی آسیب‌پذیری‌های شبکه را می‌توان در این مسئله دانست که مشخص کردن ابعاد امنیتی مورد مخاطره، هم به لحاظ ارزیابی ضعف امنیتی موجود در یک شبکه و هم از جهت تعیین اقدامات امنیتی لازم در برخورد با آسیب‌پذیری قابل توجه است.

نکته قابل توجه دیگر در انتخاب جنبه‌های امنیتی معماری امنیت ITU-TX-805 به عنوان ساختار تعیین فعالیت‌های در معرض آسیب‌پذیری در ارائه روش کمی‌سازی آسیب‌پذیری‌ها در این تحقیق، ماهیت چندوجهی رخداد هر آسیب‌پذیری است. به عبارت دیگر، ممکن است یک آسیب‌پذیری بیش از یک بُعد امنیتی را به مخاطره اندازد، یا مربوط به چند نوع فعالیت باشد و یا حتی بیش از یکی از اجزاء شبکه را شامل شود. این مسئله در حالی است که امروزه بیشتر آسیب‌پذیری‌ها به صورت ترکیبی بوده و به عبارتی با در کنار هم قرار گرفتن دو سرویس خاص و یا گاهی یک سرویس در کنار یکی از عناصر زیرساخت شبکه یا کاربرد خاص ایجاد مشکل می‌کند. به منظور محاسبه کمی آسیب‌پذیری‌های شبکه در بُعد جنبه‌های امنیتی برای ساختار مورد استفاده در این تحقیق، از سیستم امتیازدهی آسیب‌پذیری متعارف (CVSS) که در سال ۲۰۰۷ توسط مجمع واکنش به وقایع و گروه‌های امنیتی (FIRST) ارائه گردیده، استفاده شده است.

سیستم امتیازدهی آسیب‌پذیری متعارف (CVSS) از سه گروه معیار تحت عناوین (۱) معیارهای اساسی (پایه‌ای)، (۲) معیارهای موقتی و (۳) معیارهای محیطی تشکیل شده است که هر یک از این گروه معیارها نیز به نوبه خود شامل مجموعه‌ای از زیرمعیارهای دیگر

می باشد. معیارهای پایه ای، ویژگی های اصلی و پایه ای یک آسیب پذیری هستند که در طول زمان ثابت بوده و به محیط کاربر بستگی ندارند. در مقابل، معیارهای موقتی با گذشت زمان تغییر می کنند، ولی بین محیط های کاربری مختلف یکسان هستند. معیارهای محیطی نیز به یک محیط خاص کاربری مربوط بوده و منحصر به آن محیط می باشند (Mell et al 2006).

از ویژگی های روش CVSS سادگی و سهولت درک آن است. در این روش، وقتی که به معیارهای پایه ای مقادیر مناسبی اختصاص داده شود، معادله پایه ای، مقداری بین ۰ تا ۱۰ خواهد گرفت. استفاده از معیارهای موقتی و محیطی اختیاری است، ولی می توان با تخصیص مقادیر مناسب به این معیارها امتیاز پایه را پالایش کرد. استفاده از معیارهای موقتی و محیطی میزان ریسک ناشی از آسیب پذیری را با دقت بیشتری منعکس می سازد، اما استفاده از این معیارها الزامی نیست و با توجه به هدف، ممکن است استفاده از امتیاز پایه کافی باشد (همان).

تاکنون مطالعات متعددی به منظور متناسب سازی مدل پایه CVSS برای سازمان ها و محاسبه آسیب پذیری ها برای مقاصد مختلف و همچنین افزایش کارایی مدل پایه انجام شده است. به عنوان نمونه می توان به مطالعات زیر اشاره کرد: تعیین نقاط کارآمدی و ناکارآمدی مدل CVSS و متناسب سازی آن (Scarfone et al 2009; Mell et al 2007)؛ لزوم بومی سازی مدل پایه CVSS در سازمان های مختلف و اهمیت بومی سازی مدل به منظور بهره مندی از مزایای آن (Fruhirth and Mannisto 2009)؛ بررسی اثرات معیارهای محیطی بر کارآمدی مدل CVSS و ارائه راهکارهایی به منظور تأثیردهی دقیق معیارهای محیطی به عنوان عامل اصلی در بومی سازی مدل (Gallon 2010)؛ و اهمیت معیارهای محیطی در متناسب سازی مدل پایه CVSS و نقش معیار توزیع هدف به عنوان یک معیار متناسب کننده در تأثیردهی شرایط محیطی سازمان ها در فرایند محاسبه مؤثر این روش (Harada et al 2010).

«هامب» و «فرانکریا» نیز به ارائه مدلی به منظور پیش بینی میزان احتمال رخداد آسیب پذیری و ریسک حاصل از آن در سازمان ها بر اساس مدل CVSS پرداخته اند (Houmb and Franqueira 2009). در این تحقیق با ارائه دو شاخص تکرار سوء استفاده و اثر

سوءاستفاده از آسیب پذیری‌ها به پیش‌بینی آسیب‌پذیری‌ها بر اساس فرایند «مارکوف»^۱ اقدام گردیده که بر اساس پیش‌بینی انجام‌شده امکان تبدیل آسیب‌پذیری‌ها به خدمات لازم برای مقابله با آسیب‌پذیری‌ها فراهم می‌گردد. در این تحقیق، شاخص تکرار سوءاستفاده از آسیب‌پذیری‌ها بر اساس معیارهای پایه و موقتی و شاخص اثر سوءاستفاده از آسیب‌پذیری‌ها بر اساس معیارهای پایه و محیطی مورد محاسبه قرار گرفته است. از مقایسه مشخصه‌های مورد استفاده در معیارهای پایه‌ای سیستم امتیازدهی متعارف با ساختار جنبه‌های امنیتی معماری امنیت ITU-TX-805 می‌توان به این نتیجه رسید که معیارهای پایه‌ای سیستم امتیازدهی متعارف با جنبه‌های امنیتی معماری امنیت ITU-TX-805 تطابق نزدیکی داشته و می‌توان با اعمال تغییراتی نسبت به متناسب‌سازی سیستم امتیازدهی متعارف برای محاسبه آسیب‌پذیری‌های شبکه اقدام نمود. روش پیشنهادی در این تحقیق سیستم امتیازدهی آسیب‌پذیری متعارف شبکه^۲ (NCVSS) نامیده شده است. جدول شماره ۳ به مقایسه مؤلفه‌های جنبه‌های امنیتی شبکه معماری امنیت ITU-TX-805 با معیارهای پایه مندرج در مدل CVSS پرداخته است. همان‌گونه که از این جدول مشخص می‌گردد، در تطابق میان مؤلفه‌های رده‌بندی پیشنهادی و معیارهای پایه در زمینه مؤلفه عدم انکار و امنیت ارتباطات در معیارهای پایه‌ای سیستم امتیازدهی متعارف معیاری وجود ندارد. به این منظور در روش پیشنهادی NCVSS این مسئله با اعمال دو متغیر جدید در معیارهای پایه به صورت جدول شماره ۴ پوشش داده شده است.

1. Markov
2. Network Common Vulnerability Scoring System

جدول ۳. تطابق مؤلفه‌های ساختار جنبه‌های امنیتی شبکه و معیارهای پایه CVSS

مؤلفه‌های ساختار جنبه‌های امنیتی شبکه معماری امنیت ITU-TX- 805	معیارهای پایه‌ای مندرج در CVSS
کنترل دسترسی	بردار دسترسی (AV)
احراز هویت	تصدیق اصالت (AU)
عدم انکار	----
محرمانگی داده‌ها	تأثیر بر محرمانگی (C)
امنیت ارتباطات	-----
تمامیت داده	تأثیر جامعیت (I)
قابلیت دسترسی	پیچیدگی دسترسی (AC)
حریم خصوصی	تأثیر در دسترس پذیری (A)

جدول ۴. معیارهای پایه مؤلفه‌های روش NCVSS و تطابق آن با مؤلفه‌های ساختار جنبه‌های امنیتی

معماری امنیت ITU-TX- 805

مؤلفه‌های ساختار جنبه‌های امنیتی معماری امنیت ITU-TX- 805	معیارهای پایه‌ای NCVSS
کنترل دسترسی	بردار دسترسی (AV)
احراز هویت	تصدیق اصالت (AU)
عدم انکار	تصدیق فعالیت (AA)
محرمانگی داده‌ها	تأثیر بر محرمانگی (C)
امنیت ارتباطات	تأثیر بر امنیت ارتباطات (CS)
تمامیت داده	تأثیر جامعیت (I)
قابلیت دسترسی	پیچیدگی دسترسی (AC)
حریم خصوصی	تأثیر در دسترس پذیری (A)

بر اساس موارد اشاره شده، معیارهای پایه‌ای و مشخصه‌های آن بر پایه مدل CVSS به منظور استفاده در موضوع این مقاله در قالب روش NCVSS به صورت جدول شماره ۵ پیشنهاد شده است. همان گونه که از این جدول برمی آید، در مقایسه مدل CVSS با روش

NCVSS پیشنهادی دو معیار تصدیق فعالیت و تأثیر بر امنیت ارتباطات به جدول معیارهای پایه اضافه گردیده و مشخصه این معیارها و توضیحات مربوط به آنها در جدول شماره ۵ درج گردیده است. سایر معیارهای پایه در روش NCVSS مشابه مدل CVSS می باشد. در خصوص معیارهای موقتی و معیارهای محیطی نیز، معیارها و مشخصه های مربوطه در روش پیشنهادی NCVSS مشابه موارد مندرج در مدل CVSS می باشد. معیارهای موقتی و محیطی و مشخصه های آنان در جداول شماره ۶ و ۷ ارائه شده است. مشخصه ها و مقادیر کمی مربوطه بر مبنای مدل CVSS می باشد.

جدول ۵. معیارهای پایه در روش NCVSS

معیار	مشخصه	مقدار کمی	توضیح
در دسترس می	شبکه LAN داخلی	۰/۳۹۵	در آسیب پذیری که فقط با دسترسی محلی قابل بهره برداری است، حمله کننده به دسترسی فیزیکی به سیستم آسیب پذیر با یک حساب محلی نیاز دارد.
	بی سیم W-LAN شبکه اینترنت	۰/۴۶۴ ۱	حمله کننده باید در دامنه شبکه بی سیم قرار داشته باشد. در آسیب پذیری قابل بهره بردای از راه شبکه اینترنت، حمله کننده نیاز به دسترسی به شبکه LAN و یا قرار گرفتن در دامنه شبکه ندارد.
تجدید دسترسی	زیاد (H)	۰/۳۵	شرایط دسترسی لازم است. در این موارد حمله کننده باید دارای مهارت های سطح بالا باشد، اطلاعات مورد نیاز جهت فعالیت به صورت دستی قابل دستیابی نبوده و حمله کننده باید نرم افزارهای تخصصی را در اختیار داشته باشد.
	متوسط (M)	۰/۶۱	شرایط دسترسی تا حدی تخصصی هستند. در این موارد حمله کننده باید دارای مهارت بوده و اطلاعاتی را از درون شبکه جمع آوری نماید تا بر اساس آن عمل کند. شبکه فاقد تنظیمات پیش فرض است.
	کم (L)	۰/۷۱	شرایط دسترسی تخصصی وجود ندارد. در این حالت نیاز به مهارت کمی وجود دارد و به صورت دستی و بدون استفاده از نرم افزارهای خاص نفوذ به شبکه امکان پذیر باشد و به اطلاعات اضافی جهت بهره بردای از شبکه نیازی نیست.

معیار	مشخصه	مقدار کمی	توضیح
تصدیق اصالت	متعدد (M)	۰/۴۵	حمله کننده برای بهره برداری از آسب پذیری باید دو بار یا بیشتر تصدیق اصالت کند (حتی اگر از همان شناسه کاربر و کلمه عبور استفاده شود).
	واحد (S)	۰/۵۶	یک تصدیق اصالت برای دسترسی و بهره برداری از آسب پذیری نیاز است.
	هیچ (N)	۰/۷۴	برای بهره برداری از آسب پذیری به تصدیق اصالت نیاز نیست
تصدیق فعالیت	متعدد (M)	۰/۴۵	راه های متعددی برای اثبات فعالیت های انجام شده در سیستم وجود دارد
	واحد (S)	۰/۵۶	یک راه برای تصدیق فعالیت های انجام شده وجود دارد
	هیچ (N)	۰/۷۰۴	هیچ راهی به منظور جلوگیری از انکار وجود ندارد
تأثیر بر محرمانگی	هیچ (N)	۰	هیچ تأثیری روی محرمانگی سیستم ندارد.
	ناقص (P)	۰/۲۷۵	افشاء اطلاعات قابل توجهی وجود دارد و دسترسی به برخی فایل های سیستم امکان پذیر است، ولی حمله کننده کنترل روی چیزی که به دست می آورد، ندارد یا حوزه زیان، محدوده شده است به عنوان مثال، می توان به آسب پذیری که فقط می تواند جداول خاصی از پایگاه داده را افشاء سازد، اشاره کرد.
	کامل (C)	۰/۶۶	همه فایل های سیستم افشاء شده اند و حمله کننده می تواند همه داده های سیستم را بخواند.
تأثیر بر امنیت ارتباطات	متعدد (M)	۰/۴۵	لایه های متعددی برای ایجاد امنیت ارتباطات وجود دارد.
	واحد (S)	۰/۵۶	یک لایه برای ایجاد امنیت ارتباطات وجود دارد.
	هیچ (N)	۰/۷۰۴	هیچ راهکاری جهت امن سازی ارتباطات وجود ندارد.

معیار	مشخصه	مقدار کمی	توضیح
فایلین مقیاس پذیر	هیچ (N)	۰	تأثیری روی جامعیت اطلاعات ندارد (هیچ گونه تغییری در اطلاعات و یا فایل های موجود بر روی سیستم فعال در شبکه ایجاد نمی شود)
	ناقص (P)	۰/۲۷۵	تغییر برخی فایل ها یا اطلاعات ممکن است، ولی حمله کننده کنترل روی آنچه می تواند تغییر داده شود، ندارد یا حوزه ای که حمله کننده می تواند آن را تحت تأثیر قرار دهد، محدود است.
در دسترس پذیر	کامل (C)	۰/۶۶	حمله کننده می تواند هر فایلی را تغییر دهد.
	هیچ (N)	۰	تأثیری بر دسترسی پذیری سیستم ندارد.
	ناقص (P)	۰/۲۷۵	در دسترس کاربران مجاز وقفه هایی ایجاد نموده و یا کارایی آنها را کاهش می دهد.
	کامل (C)	۰/۶۶	بر اثر حمله، دسترسی سایرین به شبکه قطع می شود.

جدول ۶. معیارهای موقتی در روش NCVSS

معیار	مشخصه	مقدار کمی	توضیح
فایلین مقیاس پذیر	اثبات نشده (U)	۰/۸۵	نرم افزار یا ابزاری وجود ندارد و یا وجود آن در حد تئوری است.
	اثبات مفهوم (POC)	۰/۹	کدها یا تکنیک ها در همه موقعیت ها عملی نیست و ممکن است به تغییرات اساسی توسط حمله کننده نیاز داشته باشد.
	در حال کار (F)	۰/۹۵	ابزارها و نرم افزارهایی در دسترس است و در بسیاری از موقعیت هایی که آسیب پذیری وجود دارد، قابل استفاده و کاربری است.
	زیاد (H)	۱	ابزارها و نرم افزارهای گسترده و فراگیر به همراه جزئیات آنها در دسترس همه قرار دارد و استفاده از آن ساده و پُر کاربرد است.
	تعریف نشده (ND)	۱	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تأثیری نخواهد گذاشت.

معیار	مشخصه	مقدار کمی	توضیح
معیار معیاری	ترمیم آسیب پذیری رسمی (OF)	۰/۸۷	سازمان، یک راه حل رسمی و تعریف شده دارد.
	ترمیم آسیب پذیری موقتی (TF)	۰/۹	سازمان، نسبت به تأمین یک راه حل موقتی اقدام نماید.
	دور زدن آسیب پذیری (W)	۰/۹۵	سازمان، نیازمند صرف وقت برای تعیین یک راه حل احتمالی جهت حل موضوع است، اما مسئله قابل حل می باشد.
اطمینان از گزارش	غیر قابل دسترس (U)	۱	راه حلی در دسترس نیست یا به کار بردن آن غیرممکن است.
	تعریف نشده (ND)	۱	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تأثیری نخواهد گذاشت.
	تأیید نشده (UN)	۰/۹	فقط یک منبع تأیید نشده آسیب پذیری را گزارش کرده است یا چندین گزارش متناقض وجود دارد که این گزارشات نیز اعتبار زیادی ندارند.
	اثبات نشده (UR)	۰/۹۵	چندین منبع غیررسمی مانند سازمان های امنیتی و تحقیقاتی گزارشاتی داده اند و ممکن است بین جزئیات فنی این گزارش ها تناقض وجود داشته باشد.
	تأیید شده (C)	۱	آسیب پذیری توسط مراجع ذیصلاح تأیید شده است.
	تعریف نشده (ND)	۱	با تخصیص این مقدار به معیار در محاسبه امتیاز نهایی تأثیری نخواهد گذاشت.

به منظور کمی سازی نتایج و امتیازدهی به آسیب پذیری ها نیز معادلات پایه مدل CVSS در قالب روش NCVSS مورد بازنگری قرار گرفته است. بر این اساس دو معیار تصدیق فعالیت و تأثیر بر امنیت ارتباطات به ساختار محاسبه مدل CVSS اضافه گردیده است. همچنین در روش NCVSS معادله موقتی و محیطی مشابه موارد مندرج در مدل CVSS مورد استفاده واقع شده است. شکل شماره ۲ ساختار محاسباتی معادلات پایه، موقتی و محیطی در روش پیشنهادی NCVSS را نمایش می دهد.

جدول ۷. معیارهای محیطی در روش NCVSS

معیار	مشخصه	مقدار کمی توضیح
میزان خسارت بالقوه	هیچ (N)	امکان وارد آمدن خسارت و یا کاهش بازده و کارآیی وجود ندارد.
	کم (L)	بهره برداری موفق از آسیب پذیری خسارت فیزیکی یا مالی کمی دارد یا روی کارآیی یا بازدهی تأثیر کمی می گذارد.
	کم - متوسط (LM)	بهره برداری موفق از آسیب پذیری خسارت فیزیکی یا مالی متوسط دارد یا روی کارآیی یا بازدهی تأثیر متوسط دارد.
	متوسط - زیاد (MH)	بهره برداری موفق از آسیب پذیری خسارت فیزیکی یا مالی مهمی دارد یا روی کارآیی یا بازدهی تأثیر مهمی می گذارد.
	زیاد (H)	بهره برداری موفق از آسیب پذیری خسارت فیزیکی یا مالی فاجعه باری دارد یا روی کارآیی یا بازدهی تأثیر فاجعه بار می گذارد.
	تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار در محاسبه امتیاز نهایی تأثیری نخواهد گذاشت.
وزن هدف	هیچ (N)	هیچ سیستم هدفی وجود ندارد یا اهداف بسیار تخصصی هستند و فقط در محیط آزمایشگاه وجود دارند، یعنی ۱۰ درصد از محیط در معرض ریسک قرار دارد.
	کم (L)	اهداف در یک مقیاس کم در داخل محیط وجود دارند. بین ۲۵ الی ۱ درصد از کل محیط در معرض ریسک قرار دارد.
	متوسط (M)	اهداف در یک مقیاس متوسط در داخل محیط وجود دارند. بین ۷۵ الی ۲۶ درصد کل محیط در معرض ریسک قرار دارد.
	زیاد (H)	اهداف در یک مقیاس قابل توجه در داخل محیط وجود دارند. بین ۱۰۰ الی ۷۶ درصد کل محیط در معرض ریسک قرار دارد.
	تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تأثیری نخواهد گذاشت.

معیار	مشخصه	مقدار کمی توضیح
تأثیر پذیری	کم (L)	از بین رفتن محرمانگی، جامعیت، در دسترس پذیری تأثیر محدودی روی سازمان و افرادی که با آن در ارتباط هستند (کارکنان، مشتریان) می گذارد.
	متوسط (M)	از بین رفتن محرمانگی، جامعیت، در دسترس پذیری تأثیر سنگینی روی سازمان و افرادی که با آن در ارتباط هستند (کارکنان، مشتریان) می گذارد.
	زیاد (H)	از بین رفتن محرمانگی، جامعیت، در دسترس پذیری تأثیر فاجعه انگیزی روی سازمان و افرادی که با آن در ارتباط هستند (کارکنان، مشتریان) می گذارد.
	تعریف نشده (ND)	با تخصیص این مقدار به معیار، این معیار روی امتیاز تأثیری نخواهد گذاشت.

۴-۲. جامعه آماری و نمونه آماری

جامعه آماری مورد استفاده در این تحقیق را خبرگان، متخصصان و کارشناسان حوزه امنیت اطلاعات و شبکه تشکیل می دهند. در این پژوهش از آنجا که به نظرات مجموعه ای از خبرگان برای ارزیابی شاخص های چارچوب پیشنهادی تحقیق نیاز بوده، از روش نمونه گیری قضاوتی (تخصصی) استفاده شده است. نمونه گیری قضاوتی مستلزم گزینش بخشی از جامعه است که اعضای آن بر پایه داوری شخص پژوهنده مشخص می شود (دانایی فر و دیگران ۱۳۸۷). این روش در پی جمع آوری داده ها و دیدگاه های افرادی است که در ارتباط با موضوع مورد بررسی دارای آگاهی و تجربه مؤثر می باشند. معیارهای نمونه گیری قضاوتی در این پژوهش عبارتند از: تجربه کاری در حوزه امنیت اطلاعات و شبکه، تدریس در مراکز علمی و دانشگاهی در زمینه موضوع مورد نظر، ارائه تألیفات علمی (مقاله، پایان نامه، کتاب) در حوزه مربوط. بر اساس روش نمونه گیری قضاوتی، ۷۵ نفر با مشخصات اشاره شده شناسایی گردیده و از طریق حضوری و پست الکترونیک تعداد ۷۵ نسخه پرسشنامه میان این افراد توزیع گردید که در نهایت تعداد ۴۰ پرسشنامه جمع آوری شده و در تحلیل ها مورد استفاده قرار گرفت (نرخ بازگشت پرسشنامه برابر ۵۳/۳ درصد).

۳-۴. روایی و پایایی

برای حصول اطمینان از روایی پرسشنامه، ویرایش اولیه آن جهت اخذ نظر به پنج تن از استادان صاحب نظر در حوزه فناوری و امنیت اطلاعات و شبکه ارسال و پس از اعمال اصلاحات لازم مورد استفاده قرار گرفت. به منظور تعیین پایایی پرسشنامه نیز روش آلفای کرونباخ به کار رفت. با استفاده از نرم افزار SPSS آلفای کرونباخ مجموعه سؤال های پرسشنامه برابر با ۰/۸۱۵ محاسبه گردیده که دلالت بر پایایی بالای سؤالات پرسشنامه دارد. سپس برای همگرایی در چارچوب ساختاری برای هر یک از مجموعه شاخص های انتخابی نیز به طور مجزا مقدار آلفای کرونباخ محاسبه گردید. در این مرحله نیز مقادیر به دست آمده بیشتر از حد قابل قبول ۰/۷ (Nunnally et al 1994) بود. مقادیر مربوط به هر یک از زیر مجموعه ها در جدول شماره ۸ نمایش داده شده است.

جدول ۸. چارچوب نظری تحقیق

معیار	توضیحات	
مؤلفان و موضوعات	بردار دسترسی	شناسایی چگونگی دستیابی و بعد فاصله حمله کننده برای دسترسی به شبکه
	پیچیدگی دسترسی	میزان مهارت و استعداد مورد نیاز برای بهره برداری از اطلاعات، محیط و سیستم های موجود در شبکه پس از به دست آوردن دسترسی
	تصدیق اصالت	تعداد دفعاتی که حمله کننده باید پیش از دسترسی به هدف و بهره برداری از آن تصدیق اصالت کند
	تصدیق فعالیت	تعداد و تنوع روش های قابل استفاده برای عدم انکار فعالیت های انجام شده در شبکه
	تأثیر بر محرمانگی	میزان اثر بهره بردای موفق از یک آسیب پذیری شبکه بر افشا و استفاده از اطلاعات محرمانه در محیط شبکه
	تأثیر بر امنیت ارتباطات	تعداد لایه های امنیتی که برای ایجاد امنیت ارتباطات به کار برده می شود
	تأثیر جامعیت	میزان تغییری که حمله کننده می تواند در اطلاعات، محیط و سیستم های موجود در شبکه پس از به دست آوردن دسترسی اعمال نماید
	در دسترس پذیری	میزان تغییری که حمله کننده می تواند در دسترسی کاربران به شبکه پس از نفوذ به شبکه اعمال نماید

معیار	توضیحات
معیارهای موثقی	قابلیت بهره‌برداری سطح ترمیم
	میزان دسترسی عمومی به نرم‌افزارها، کدها و تکنیک‌هایی که برای نفوذ و آسیب‌رسانی به شبکه‌ها قابل استفاده است راهکارهای سازمانی در جهت مدیریت و مواجهه با آسیب‌های ایجادشده
	میزان اطمینان از وجود آسیب‌پذیری و اعتبار جزئیات فنی آن گزارش
معیارهای محیطی	میزان خسارت ناشی از حمله و یا دسترسی غیرمجاز به شبکه (شامل انواع خسارت اقتصادی، کارآیی، بازده و ...)
	میزان خسارت ناشی از حمله و یا دسترسی غیرمجاز به شبکه (شامل انواع خسارت اقتصادی، کارآیی، بازده و ...)
	میزان سیستم‌هایی که می‌توانند توسط آسیب‌پذیری واردشده به شبکه تحت تأثیر قرار گیرند
نیازهای امنیتی	میزان تأثیر از بین رفتن امنیت در ابعاد جامعیت، دسترسی و محرمانگی بر سازمان و افراد مرتبط با آن (کارکنان، مشتریان)

۴-۴. تحلیل داده‌ها

بررسی متغیرهای جمعیت‌شناختی پاسخ‌دهندگان به سؤالات پرسشنامه نشان می‌دهد که ۲۸/۴ درصد از پاسخ‌دهندگان زن و ۷۱/۶ درصد مرد می‌باشند. همچنین از نظر سطح تحصیلات ۱۹ درصد دارای مدرک کارشناسی، ۶۱/۳ درصد دارای مدرک کارشناسی ارشد و ۱۹/۷ درصد دارای مدرک دکترا هستند. از نظر بررسی هرم سنی مشخص می‌گردد که ۲۶/۴ درصد از پاسخ‌دهندگان در رده سنی ۲۵-۳۵ سال، ۴۴/۳۶ درصد در رده سنی ۳۵-۴۵ سال و ۲۹/۲۴ درصد در رده سنی بالای ۴۵ سال قرار دارند.

با به‌کارگیری روش آماری تحلیل عاملی و با توجه به نتایج به‌دست آمده برای آزمون شاخص کیفیت نمونه‌گیری ($KMO=0/653$) که بزرگتر از مقدار قابل قبول ۰/۶ (Hair 1998) بوده و عدد معناداری آزمون بارتلت ($sig=0/00$) که کمتر از ۰/۰۵ است، می‌توان تناسب داده‌ها برای اجرای تحلیل عاملی و کافی بودن اندازه نمونه گرفته‌شده را استنباط کرد. نتایج حاصل از تحلیل عاملی و آمار توصیفی داده‌ها در جدول شماره ۹ ارائه گردیده است. بر اساس محاسبات واریانس کل تبیین‌شده برابر با ۶۱/۹۸ درصد می‌باشد. بدین معنی که معیارهای مورد بررسی این میزان از آسیب‌پذیری‌های شبکه را شناسایی می‌کنند. این مقدار نشان‌دهنده روایی مناسب سؤالات این حوزه نیز می‌باشد. همان‌طور که جدول شماره ۹ نشان می‌دهد تمامی معیارها دارای بار عاملی بیش از ۰/۵ می‌باشند. بر

اساس محاسبات مندرج در همین جدول، معیارهای پایه‌ای بیشترین نقش را در تبیین واریانس به خود اختصاص داده و معیارهای موقتی و معیارهای محیطی به ترتیب در اولویت‌های بعدی قرار می‌گیرند. از آنجا که بارهای عاملی سؤالات با عامل مربوط به خود بالای ۰/۵۰ و با عامل‌های دیگر کمتر از ۰/۵۰ می‌باشد، روایی و اگر نیز حاصل شده است (صدقی و دیگران ۱۳۸۸). بر اساس نتایج اجرای تحلیل عاملی، آن‌گونه که در جدول شماره ۹ نمایان است، معیارهای پایه‌ای بیشترین نقش را در تبیین واریانس آسیب‌پذیری‌های شبکه دارا می‌باشند (واریانس تبیین شده = ۳۰/۱۴۳) و معیارهای موقتی (واریانس تبیین شده = ۱۶/۰۲۸) و معیارهای محیطی (واریانس تبیین شده = ۱۵/۸۱۱) دارای اولویت‌های بعدی هستند.

جدول ۹. نتایج تحلیل داده‌ها

آلفای کروباخ	وارانس تبیین شده	ارزش ویژه	بار عاملی			معیار	معیار	معیار	
			عامل سوم	عامل دوم	عامل اول				
۰/۸۷	۳۰/۱۴۳	۴/۵۱۴	۰/۱۹۶	۰/۱۳۴	۰/۷۰۳	۱/۰۳۲	۳/۱	بردار دسترسی	معیارهای پایه‌ای (میانگین = ۳/۰۹، انحراف معیار = ۰/۷۲)
			۰/۰۱۶	-۰/۰۷۵	۰/۶۸۲	۱/۰۸۶	۳	پیچیدگی دسترسی	
			۰/۳۷۲	۰/۲۴۲	۰/۸۰۵	۱/۱۲۸	۲/۴	تصدیق اصالت	
			۰/۲۲۱	۰/۱۷۴	۰/۶۹۷	۰/۹۰۴	۲/۵۵	تصدیق فعالیت	
			۰/۱۶۸	-۰/۱۳۲	۰/۸۵۷	۱/۰۸۱	۲/۹	تأثیر بر محرمانگی	
			-۰/۴۰۸	-۰/۱۸۳	۰/۵۵۹	۰/۹۴۹	۳/۶۵	تأثیر بر امنیت ارتباطات	
			-۰/۲۲۸	-۰/۱۴۶	۰/۶۱۵	۰/۸۹۱	۳/۹۸	تأثیر جامعیت	
			۰/۲۱۸	-۰/۱۵۲	۰/۷۹۴	۰/۹۳۱	۳/۱۷۵	در دسترس پذیری	
۰/۷۱	۱۵/۸۱۱	۱/۸۷۳	۰/۶۹۵	۰/۰۴۶	۰/۱۲۳	۱/۱۰۲	۳/۶۲	قابلیت بهره‌برداری	معیارهای موقتی (میانگین = ۳/۰۶۲، انحراف معیار = ۰/۸۲)
			۰/۸۲	-۰/۰۷۴	۰/۱۵۵	۰/۸۷۷	۳/۷۲	سطح ترمیم	
			۰/۷۱۳	-۰/۰۸۳	۰/۰۹۱	۱۱/۰۸۶	۳/۵	اطمینان از گزارش	
۰/۷۹	۱۶/۰۲۸	۲/۲۹۰	-۰/۰۱۳۸	۰/۸۹۵	۰/۰۱۳	۱/۲۵	۳/۷۷	میزان خسارت بالقوه	معیارهای محیطی (میانگین = ۳/۰۹، انحراف معیار = ۰/۹۴)
			۰/۰۹۴	۰/۸۴۲	-۰/۱۴۸	۱/۲۶۵	۳/۷	توزیع هدف	
			-۰/۰۸	۰/۷۱۸	۰/۰۳۹	۰/۸	۴/۲۲۵	نیازهای امنیتی	

بر اساس موارد مندرج در جدول شماره ۹ مشاهده می‌گردد که میانگین تمامی ابعاد بیشتر از عدد ۳ می‌باشد و این مقدار نشان دهنده پاسخ مثبت به ابعاد است. بر اساس نتایج حاصل از تحلیل عاملی درج شده در جدول شماره ۹ مشخص می‌گردد که بار عاملی

تمامی معیارهای مورد آزمون بیشتر از ۰/۵ می باشد و تمامی معیارهای انتخابی در تبیین آسیب پذیری های شبکه نقش دارند. واریانس کل تبیین شده توسط ابعاد مدل برابر با ۶۱/۹۸ درصد بوده که نشانگر مطلوبیت چارچوب پیشنهادی در تبیین آسیب پذیری های شبکه می باشد. بر اساس موارد مندرج در همین جدول، معیارهای پایه ای با بار عاملی ۳۰/۱۴۳ بیشترین نقش را در تبیین آسیب پذیری های شبکه دارا بوده و پس از آن بُعد محیطی با بار عاملی ۱۶/۰۲۸، و بُعد موقتی با بار عاملی ۱۵/۸۱۱ نقش های بعدی در تبیین آسیب پذیری های شبکه را به خود اختصاص داده اند. این مقادیر نشانگر میزان اهمیت هر یک از این ابعاد در شناسایی آسیب پذیری های شبکه می باشد. معیار میزان خسارت بالقوه از مجموعه معیارهای محیطی (با بار عاملی ۰/۸۹۵) دارای بیشترین بار عاملی و معیار تأثیر بر امنیت ارتباطات (با بار عاملی ۰/۱۸۳-) دارای کمترین بار عاملی در میان معیارهای آسیب پذیری شبکه را دارا می باشند.

۴-۵. بررسی یک نمونه عملی

در این بخش به منظور تعیین نحوه محاسبات کمی در خصوص میزان آسیب پذیری شبکه در راهکار پیشنهادی، به بررسی یک نمونه عملی پرداخته شده است. نمونه عملی مورد نظر دارای فعالیت تولیدی در عرصه صنعت کاشی و سرامیک بوده و دارای یک محیط تولیدی و دو دفتر منطقه ای می باشد. تعداد کاربران فعال که از شبکه این مجموعه استفاده می نمایند، ۱۵۳ نفر در محیط تولیدی، ۲۷ نفر در دفتر منطقه ای الف و ۵۴ نفر در دفتر منطقه ای ب می باشد. ارتباط میان این سه موقعیت جغرافیایی از طریق شبکه MPLS و ارتباطات بی سیم تأمین می گردد. این مجموعه اخیراً اقدام به تأمین سیستم های ERP تحت وب نموده که ۷۰ درصد از ماژول های سیستم خریداری شده پیاده سازی و عملیاتی شده است. این مجموعه به منظور افزایش ضریب امنیت اطلاعات سازمانی خود در نظر دارد طرحی به نام طرح جامع افزایش ضریب امنیت اطلاعات و شبکه را در سازمان خود اجرا نماید. با توجه به هماهنگی صورت پذیرفته با این مجموعه و معرفی روش پیشنهادی در این مقاله مقرر گردید در راستای اولویت بندی اجرای طرح افزایش ضریب امنیت اطلاعات سازمانی نسبت به محاسبه میزان آسیب پذیری شبکه این مجموعه برای موقعیت تولیدی و دفاتر منطقه ای اقدام گردد. بدین منظور یک جلسه هم اندیشی برای معرفی روش پیشنهادی

با حضور متخصصان واحد فناوری اطلاعات برگزار گردید. پس از این جلسه و تشریح روش، اطلاعات لازم با همکاری کارشناسان واحد فناوری اطلاعات جمع آوری شد. خلاصه نتایج به دست آمده در جدول شماره ۱۰ درج گردیده است.

جدول ۱۰. مقادیر متغیرهای مربوط به معیارهای پایه، موقتی و محیطی در نمونه مورد بررسی

دفتر منطقه ای ب		دفتر منطقه ای الف		محیط تولیدی		معیار	
مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه		
۱	شبکه LAN داخلی	۰/۶۴۶	شبکه LAN داخلی	۱	شبکه LAN داخلی	بردار دسترسی	معیارهای پایه
	بی سیم W-LAN		شبکه اینترنت		شبکه اینترنت		
	شبکه اینترنت LAN		شبکه اینترنت		شبکه اینترنت		
۰/۶۱	متوسط (M)	۰/۶۱	متوسط (M)	۰/۳۵	زیاد (H)	پیچیدگی دسترسی	
۰/۵۶	واحد (S)	۰/۵۶	واحد (S)	۰/۵۶	واحد (S)	تصدیق اصالت	
۰/۵۶	واحد (S)	۰/۵۶	واحد (S)	۰/۵۶	واحد (S)	تصدیق فعالیت	
۰/۲۷۵	ناقص (P)	۰/۲۷۵	ناقص (P)	۰/۲۷۵	ناقص (P)	تأثیر بر محرمانگی	
۰/۵۶	واحد (S)	۰/۵۶	واحد (S)	۰/۵۶	واحد (S)	تأثیر بر امنیت ارتباطات	
۰	هیچ (N)	۰	هیچ (N)	۰/۲۷۵	ناقص (P)	تأثیر جامعیت	
۰/۶۶	کامل (C)	۰/۶۶	کامل (C)	۰/۲۷۵	ناقص (P)	در دسترس پذیری	
۰/۹۵	در حال کار (F)	۰/۹۵	در حال کار (F)	۰/۹۵	در حال کار (F)	قابلیت بهره برداری	معیارهای ثانویه

دفتر منطقه ای ب		دفتر منطقه ای الف		محیط تولیدی		معیار
مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه	
۰/۸۷	ترمیم آسیب پذیری موقتی (TF)	۰/۸۷	ترمیم آسیب پذیری رسمی (OF)	۰/۹۵	دور زدن آسیب پذیری (W)	سطح ترمیم
۱	تعریف نشده (ND)	۱	تعریف نشده (ND)	۱	تعریف نشده (ND)	اطمینان از گزارش
۱	متوسط - زیاد (MH)	۰,۱	کم (L)	۰/۴	متوسط - زیاد (MH)	میزان خسارت بالقوه
۰	هیچ (N)	۰	هیچ (N)	۰/۲۵	کم (L)	توزیع هدف
۰/۲۵	کم (L)	۰,۵	کم (L)	۱	متوسط (M)	نیازهای امنیتی

با وارد نمودن مقادیر مندرج در جدول شماره ۱۰ در فرمول های محاسباتی ارائه شده در روش پیشنهادی (بر اساس نحوه محاسبه ارائه شده در شکل شماره ۲) مقادیر معیارهای پایه، موقتی و محیطی برای شبکه این مجموعه در سه موقعیت تولیدی، دفتر منطقه ای الف و دفتر منطقه ای ب محاسبه و مقادیر و محاسبات آن در شکل شماره ۳ درج گردید.

مقادیر معیارهای پایه، موقتی و محیطی در محیط تولیدی
<p>BaseScore = round_to_1_decimal (((0.6*6.443) + (0.4*1.229)-1.5)*1.176) = 3.4 Impact = 10.41*(1-(1-0.275)*(1-0.275)*(1-0.275)) = 6.443 Exploitability = 20*1*0.35*0.56*0.56*0.56 = 1.229 f (impact) = 1.176</p> <p>TemporalScore = round_to_1_decimal (3.4*0.95*0.95*1) = 3.1 EnvironmentalScore = round_to_1_decimal (5.23 + (10-5.23)*0.4*0.25) = 1.8 AdjustedImpact = min (10, 10.41*(1-(1-0.275*1)*(1-0.275*1)*(1-0.275*1))) = 6.44 AdjustedBase = (((0.6* 6.44) + (0.4* 6.44)-1.5)*1.176) = 5.8 AdjustedTemporal = (5.8 * 0.95 * 0.95 * 1) = 5.23</p>
مقادیر معیارهای پایه، موقتی و محیطی در دفتر منطقه‌ای الف
<p>BaseScore = round_to_1_decimal (((0.6*7.84) + (0.4*1.38)-1.5)*1.176) = 4.4 Impact = 10.41*(1-(1-0.275)*(1-0)*(1-0.66)) = 7.84 Exploitability = 20*0.646*0.61*0.56*0.56*0.56 = 1.38 f (impact) = 1.176</p> <p>TemporalScore = round_to_1_decimal (4.4*0.95*0.87*1) = 3.6</p> <p>* با توجه به اینکه میزان توزیع هدف برابر هیچ (N) می‌باشد، محاسبه معیار محیطی لازم نمی‌باشد.</p>
مقادیر معیارهای پایه، موقتی و محیطی در دفتر منطقه‌ای ب
<p>BaseScore = round_to_1_decimal (((0.6*7.84) + (0.4*2.14)-1.5)*1.176) = 4.8 Impact = 10.41*(1-(1-0.275)*(1-0)*(1-0.66)) = 7.84 Exploitability = 20*1*0.61*0.56*0.56*0.56 = 2.14 f (impact) = 1.176</p> <p>TemporalScore = round_to_1_decimal (4.8*0.95*0.87*1) = 4.0</p> <p>* با توجه به اینکه میزان توزیع هدف برابر هیچ (N) می‌باشد، محاسبه معیار محیطی لازم نمی‌باشد.</p>

شکل ۳. محاسبات معیارهای پایه، موقتی و محیطی در نمونه مورد بررسی

همان‌گونه که از مقادیر محاسبه‌شده مشخص می‌شود، در شبکه نمونه مورد بررسی دفتر منطقه‌ای ب دارای بیشترین مقدار معیار پایه و موقتی و پس از آن دفتر منطقه‌ای الف قرار دارد. بر اساس محاسبات صورت گرفته، شبکه محیط تولیدی دارای کمترین مقادیر معیارهای پایه، موقتی و محیطی می‌باشد.

در بخش معیار پایه، دلیل اصلی بالابودن درجه آسیب‌پذیری شبکه دفتر منطقه‌ای ب نسبت به محیط تولیدی را می‌توان در مقادیر معیارهای پیچیدگی دسترسی و در دسترس‌پذیری دانست. در همین حال، دفتر منطقه‌ای الف به دلیل نوع بردار دسترسی که مقادیر پیچیدگی دسترسی و دسترس‌پذیری آن مشابه شرایط دفتر منطقه‌ای ب است، نسبت به دفتر منطقه‌ای ب دارای وضعیت بهتری در مقدار معیار پایه‌ای می‌باشد.

در بخش معیار موقتی نیز دلیل بالا بودن درجه آسیب پذیری شبکه دفتر منطقه ای الف و ب نسبت به محیط تولیدی را می توان در وضعیت معیار سطح ترمیم جستجو نمود. در همین حال، و با توجه به تأثیر معیار پایه در معیار موقتی، به دلیل بالاتر بودن مقدار معیار پایه در دفتر منطقه ای ب نسبت به دفتر منطقه ای الف، مقدار معیار موقتی آن نسبت به دفتر منطقه ای الف بالاتر خواهد بود. با توجه به محاسبات انجام شده می توان نتیجه گرفت که مجموعه مذکور می بایست اولویت طرح افزایش ضریب امنیت اطلاعات را برای دفاتر منطقه ای ب، الف و سپس محیط تولیدی خود اجرا نماید.

۵. نتیجه گیری

این مقاله تلاش نمود بر پایه معماری امنیت ITU-TX-805 روشی به منظور محاسبه کمی آسیب پذیری های شبکه تحت عنوان NCVSS ارائه نماید. برای دستیابی به هدف موضوع مقاله ضمن بررسی گسترده ادبیات مربوط به آسیب پذیری شبکه و مدل های مطرح برای کمی سازی مقادیر آسیب پذیری ها، پرسشنامه ای تدوین و برای ارزیابی اعتبار شاخص های استخراج شده در اختیار کارشناسان و خبرگان در حوزه امنیت قرار گرفت. نتایج اجرای تحلیل عاملی بر روی داده های به دست آمده، نشان دهنده تأثیر مؤلفه های آسیب پذیری بر روی میزان آسیب پذیری شبکه های رایانه ای است. بر اساس نتایج این تحقیق معیارهای پایه ای (شامل بردار دسترسی، پیچیدگی دسترسی، تصدیق اصالت، تصدیق فعالیت، تأثیر بر محرمانگی، تأثیر بر امنیت ارتباطات، تأثیر جامعیت، و در دسترس پذیری) بیشترین نقش را در تبیین واریانس آسیب پذیری های شبکه دارا می باشند (واریانس تبیین شده = $30/143$). از سوی دیگر، معیارهای موقتی (شامل قابلیت بهره برداری، سطح ترمیم، اطمینان از گزارش) با واریانس تبیین شده = $16/028$ و معیارهای موقتی (شامل میزان خسارت بالقوه، توزیع هدف، نیازهای امنیتی) با واریانس تبیین شده = $15/811$ در اولویت های بعدی قرار دارند.

بر اساس روش پیشنهادی در این تحقیق امکان مدیریت مؤثر آسیب پذیری ها از طریق کمی سازی مقادیر آسیب پذیری ها فراهم گردیده است. با توجه به نبود روش های محاسبه کمی آسیب پذیری ها در حوزه شبکه های رایانه ای و نیاز عملیاتی متخصصان این حوزه، روش پیشنهادی در این تحقیق می تواند در عین سادگی و سهولت استفاده به عنوان یک

روش ابتکاری کارآمد و مؤثر در محاسبه میزان آسیب پذیری های شبکه رایانه ای مورد استفاده قرار گیرد.

تشکر و قدردانی

پژوهشگران بر خود لازم می دانند از همکاری و مساعدت سرکار خانم مهندس فاطمه آل آقا که در انجام این تحقیق همکاری داشته اند، مراتب سپاس خود را اعلام نمایند.

۶. فهرست منابع

- امامی، ساره سادات و جعفرهادی جعفریان. ۱۳۸۸. محاسبه درجه آسیب پذیری سیستم ها. اولین کنفرانس حوادث و آسیب پذیری های امنیت فضای تبادل اطلاعات، تهران.
- امیدیان، علیرضا، علی نورالهی راوری و رسول جلیلی. ۱۳۸۸. دسته بندی آسیب پذیری های شناخته شده در سیستم های مدیریت پایگاه داده ها. اولین کنفرانس حوادث و آسیب پذیری های امنیت فضای تبادل اطلاعات، تهران.
- حاجیان، سارا، فرامرز هندسی، مهدی برنجکوب، سیدهادی هاشمی و پیمان گلشنی. ۱۳۸۸. ارائه یک رده بندی جدید برای آسیب پذیری های شبکه. اولین کنفرانس حوادث و آسیب پذیری های امنیت فضای تبادل اطلاعات، تهران.
- دانایی فر، حسن، سیدمهدی الوانی و عادل آذر. ۱۳۸۷. روش شناسی کمی در مدیریت: رویکردی جامع، اول. تهران: صفار.
- صدقی، عباس، سیدرضا سیدجوادین، داود مطلبی، سیدجابر حسینی و حمیدرضا یزدانی. ۱۳۸۸. بررسی مقایسه ای مدل های شاخص رضایت مشتری و ارائه مدلی برای سنجش رضایت مؤدیان مالیاتی سازمان امور مالیاتی کشور. مدیریت بازرگانی ۱ (۲): ۱۰۱-۱۱۸.
- Abbott, R., J. Chin, J. Donnelley, W. Konigsford, S. Tokubo, and D. Webb. 1976. *Security Analysis and Enhancements of Computer Operating Systems*. In: Institute for Computer Science and Technology, National Bureau of Standards; 1-62.
- Ahmad, N. H., S. A. Aljunid and J. Manan. 2011. *Understanding vulnerabilities by refining taxonomy*. In: Information Assurance and Security (IAS), 7th International Conference on, 5-8 Dec. 2011. 25-29.
- Alvi, A. K. and M. Zulkernine. 2011. *A Natural Classification Scheme for Software Security Patterns*. In: Dependable, Autonomic and Secure Computing (DASC), IEEE Ninth International Conference on, 12-14 Dec. 2011. 113-120.
- Alhazmi, OH., Y. Malaiya. 2005. *Quantitative vulnerability assessment of systems software*.

- Annual Reliability and Maintainability Symposium, 2005 Proceedings. 615-620.
- Ammala, DE. 2004. *Derivation OF Metrics for Effective Evaluation of Vulnerability Assessment Technology*. Mississippi State University.
- Ammann, P., D. Wijesekera and S. Kaushik. 2002. *Scalable, graph-based network vulnerability analysis*. In: the 9th ACM Conference on Computer and Communications Security: ACM Press; 217-224.
- Aslam, T. 1995. *A taxonomy of security faults in the UNIX operating system*. Indiana: Purdue University, West Lafayette.
- Asman, B. C., M.H. Kim, R.A. Moschitto, J.C. Stauffer, and S.H. Huddleston. 2011. *Methodology for analyzing the compromise of a deployed tactical network*. In: Systems and Information Engineering Design Symposium (SIEDS), IEEE, 29-29 April 2011. 164-169.
- Asosheh, A. and N. Ramezani. 2008. A comprehensive taxonomy of DDoS attacks and defense mechanism applying in a smart classification. *WSEAS Transactions on Computers* 7 (4): 281-290.
- Avramescu, G., M. Bucicoiu, D. Rosner, X. TA and N. Pus. 2013. *Guidelines for Discovering and Improving Application Security*. In: Control Systems and Computer Science (CSCS), 19th International Conference on, 29-31 May 2013. 560-565.
- Ben-Porat, U. 2013. Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks. *IEEE Transactions on Computers*, 62: 1031-1043.
- Bhattacharya, P. and S. K. Ghosh. 2012. Analytical framework for measuring network security using exploit dependency graph. *Information Security, IET*, 6: 264-270.
- Bisbey, R and D. Hollingworth. 1978. *Protection Analysis: Final Report*. In: ISI/SR-78-13, USC/Info. Sci. Inst: Marina Del Rey, CA.
- Bishop, M. 1995. *A Taxonomy of UNIX System and Network Vulnerabilities*. In: University of California.
- _____.1999. *Vulnerabilities Analysis*. In: Second International Symposium on Recent Advances in Intrusion Detection McGraw-Hill:125-136.
- _____.2003. *Computer security: art and science*. Boston, Mass; London: Addison-Wesley.
- Coralciuc, H. V. 2012. *A Taxonomy of Time and State Attacks*. In: Availability, Reliability and Security (ARES), Seventh International Conference on, 20-24 Aug. 2012. 564-573.
- Corona, I., G. Giacinto and F. Roli. 2013. Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues. *Information Sciences* 239: 201-225.
- Du, W and A. Mathur. 1997. *A: Categorization of Software Errors that Lead to Security Breaches*. In: COAST technical report. West Lafayette, Indiana: Department of Computer Sciences, Purdue University.
- Fruhwrth, C. and T. Mannisto. 2009. *Improving CVSS-based vulnerability prioritization and response with context information*. In: Empirical Software Engineering and Measurement, ESEM 3rd International Symposium on: 15-16 Oct.
- Gallon, L. 2010. *On the Impact of Environmental Metrics on CVSS Scores*. In: Social Computing

- (SocialCom), IEEE Second International Conference on: 20-22 Aug. 2011: 987-992.
- _____ and J. J. Bascou. 2011. *Using CVSS in Attack Graphs*. In: Availability, Reliability and Security (ARES), Sixth International Conference on, 22-26 Aug. 2011. 59-66.
- Gheorghe, AV and D. V. Vamanu. 2004. Towards QVA- Quantitative vulnerability assessment: a generic practical model. *Journal of Risk Research*, 7 (6): 613-628.
- Hair, JF. 1998. *Multivariate data analysis*. Upper Saddle River, N.J.: Prentice Hall.
- Hamed, H. and E. Al-Shaer. 2006. Taxonomy of conflicts in network security policies. *IEEE Commun Mag* 44 (3): 134-141.
- Hansman, S. and R. Hunt. 2005. A taxonomy of network and computer attacks. *Computers & Security* 24 (1): 31-43.
- Harada, T., A. Kanaoka, E. Okamoto and M. Kato. 2010. *Identifying Potentially-Impacted Area by Vulnerabilities in Networked Systems Using CVSS*. In: Applications and the Internet (SAINT), 10th IEEE/IPSJ International Symposium on: 19-23 July 2010; 367-370.
- Hernandez-Ardieta, J. L., A. I. Gonzalez-Tablas, J. M. De Fuentes. and B. Ramos. 2013. A taxonomy and survey of attacks on digital signatures. *Computers & Security*, 34: 67-112.
- Holm, H., M. Ekstedt and D. Andersson. 2012. *Empirical Analysis of System-Level Vulnerability Metrics through Actual Attacks*. Dependable and Secure Computing, IEEE Transactions on, 9, 825-837.
- Houmb, S. H. and N. L. Franqueira. 2009. *Estimating ToE Risk Level Using CVSS*. In: Availability, Reliability and Security, ARES '09 International Conference on: 16-19 March 2009 718-725.
- Howard, J D. and T. A. Longstaff. 1998. *A Common Language for Computer Security Incidents*. In: Sandia.
- Hudic, A., L. Zechner, S. Islam, C. Krieg, E.R. Weippl, S. Winkler and R. Hable. 2012. *Towards a Unified Penetration Testing Taxonomy*. In: Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on Social Computing (SocialCom), 3-5 Sept. 2012. 811-812.
- Hunt, R. and J. Slay. 2011. *A new approach to developing attack taxonomies for network security - including case studies*. In: Networks (ICON), 17th IEEE International Conference on, 14-16 Dec. 2011. 281-286.
- Jiang, F., D. DAOYI, C. LONGBING and M.R. FRATER. 2013. *Agent-Based Self-Adaptable Context-Aware Network Vulnerability Assessment*. Network and Service Management, IEEE Transactions on, 10: 255-270.
- Jungag, Y., L. Li, Y. Yanfeng and Z. Guangliang. 2012. *A Hierarchical Network Security Risk Assessment Method Based on Vulnerability Attack Link Generated*. In: Information Science and Engineering (ISISE), 2012 International Symposium on, 14-16 Dec. 2012. 113-118.
- Junshun, H., L. Xiaoyan, B. Yang and X. Chunhe. 2012. *The consistency verification of Computer Network Defense Policy and measures*. In: Information and Communication Technologies (WICT), 2012 World Congress on, Oct. -Nov. 2012. 1052-1055.
- Kakareka, A. 2013. *Chapter 31 - What is Vulnerability Assessment?* In: VACCA, J. R. (ed.) Computer and Information Security Handbook (Second Edition). Boston: Morgan

- Kaufmann.
- Kamara, S, S. Fahmy, E. Schultz, F. Kerschbaum and M. Frantzen. 2003. Analysis of vulnerabilities in Internet firewalls. *Computers & Security* 22 (3): 214-232.
- Krsul, I. V. 1998. *Software Vulnerability Analysis*. Purdue University.
- KUHN, D. R. 2011. *Vulnerability hierarchies in access control configuration*. 4th Symposium on Configuration Analytics and Automation (SAFECONFIG).
- Kundu, A., N. Ghosh, N., Chokshi, I. and Ghosh, S. K. Year. *Analysis of attack graph-based metrics for quantification of network security*. In: India Conference (INDICON), 2012 Annual IEEE, 7-9 Dec. 2012. 530-535.
- Landwehr, C. E., A. R. Bull, J. P. McDermott and W. S. Choi. 1994. A Taxonomy of Computer Program Security Flaws. *ACM Computing Surveys*, 26 (3): 211–254.
- Lough, D. L. 2001. *A Taxonomy of Computer Attacks with Applications to Wireless Networks*. Virginia Polytechnic Institute and State University; PhD thesis.
- Maatta, M. and T. Raty. 2012. *Automatic creation of models for network intrusion detection*. In: Computing, Communications and Applications Conference (ComComAp), 11-13 Jan. 2012 231-237.
- Marrone, S., R. Nardone, A. Tedesco, P. D'amore, V. Vittorini, R. Setola, F. De Cillis and N. Mazzaocca. 2013. Vulnerability modeling and analysis for critical infrastructure protection applications. *International Journal of Critical Infrastructure Protection*, 6: 217-227.
- McGee, A. R., S. R. Vasireddy, C. Xie, D. D. Picklesimer, U. Chandrashekar and S. H. Richman. 2004. A framework for ensuring network security. *Bell Labs Technical Journal* 8 (4): 7-27.
- Mell, P., K. Scarfone. 2007. Improving the Common Vulnerability Scoring System. *Information Security, IET* 1 (3): 119-127.
- ____, ____ and S. Romanosky. 2006. Common Vulnerability Scoring System. *Security & Privacy, IEEE* 4 (6): 85-89.
- Nehinbe, J. O. 2011. *Emerging threats, risks and mitigation strategies in network forensics*. In: Electrical and Computer Engineering (CCECE), 24th Canadian Conference on, 8-11 May 2011. 001228- 001232.
- Njogu, H. W., L. Jiawei, J. N. Kiere and D. Hanyurwifura. 2013. A comprehensive vulnerability based alert management approach for large networks. *Future Generation Computer Systems*, 29: 27-45.
- Nunnally, J. C., I. H. Bernstein. 1994. *Psychometric theory*, 3rd ed. New York: McGraw-Hill.
- Perla, E., O. Massimiliano and G. Speake. 2011. *A guide to kernel exploitation attacking the core* [Online]. Burlington, Mass: Syngress. [Accessed 01/09/2011].
- Pothamsetty, V. and B. A. Akyol. 2004. *A vulnerability taxonomy for network protocols: Corresponding engineering best practice countermeasures*. In: IASTED International Conference on Communications, Internet and Information Technology; Thomas, US Virgin Islands: IASTED/ACTA Press. 2004. 168-175.
- Ramakrishnan, CR. and R. Sekar. 1998. *Model-Based Vulnerability Analysis of Computer*

- Systems*. In: 2ed Int'l Workshop on Verification, Model Checking and Abstract Interpretation.
- Ristenbatt, M. P. 1988. *Methodology for network communication vulnerability analysis*. In: 21st Century Military Communications Conference. 23-26 Oct 1998; 493-499 vol. 492.
- Ryoo, J., Y. B. Choi, T. H. Oh and G. Corbin. 2009. A multi-dimensional classification framework for developing context-specific Wireless Local Area Network attack taxonomies. *International Journal of Mobile Communications* 7 (2): 253-267.
- Saxena, S. and Y. V. Hote. 2013. *Load Frequency Control in Power Systems via Internal Model Control Scheme and Model-Order Reduction*. Power Systems, IEEE Transactions on, 28, 2749-2757.
- Scarfone, K. and P. Mell. 2009. *An analysis of CVSS version 2 vulnerability scoring*. In: Empirical Software Engineering and Measurement, ESEM 3rd International Symposium on: 15-16 Oct 2009.
- Shahriar, H. and M. Zulkernine. 2011. Taxonomy and classification of automatic monitoring of program security vulnerability exploitations. *Journal of Systems and Software*, 84: 250-269.
- Shiguo, S., L. Senlin, L. Xiang. and L. Bo. 2012. *The Research on Network Vulnerability Analysis Methods*. In: Intelligent System Design and Engineering Application (ISDEA), Second International Conference on, 6-7 Jan 2012. 593-597.
- Shijia, G., L. Weihai and Z. Xin. 2011. *Brute Force Vulnerability Testing Technology Based on Data Mutation*. In: Vehicular Technology Conference (VTC Fall), IEEE, 5-8 Sept. 2011. 1-6.
- Szidarovszky, F. and L. Yi. 2011. *On optimal strategies in protecting computer networks*. In: Computer Systems and Applications (AICCSA), 9th IEEE/ACS International Conference on, 27-30 Dec. 2011. 140-143.
- Taheri, M., M. Naderi and M. Barekatin. 2010. *New approach for detection and defending the wormhole attacks in Wireless ad hoc networks*. In: Electrical Engineering (ICEE), 18th Iranian Conference on, 11-13 May, 2010. 331-335.
- Tripathi, A. and U.K. Singh. 2011. *Taxonomic analysis of classification schemes in vulnerability databases*. In: Computer Sciences and Convergence Information Technology (ICCIT), 6th International Conference on, Nov-Dec. 2011 686-691.
- Vijayakumar, A. and G. Muthuchelvi. 2011. *Discovering vulnerability to build a secured system using attack injection*. In: Electronics Computer Technology (ICECT), 2011 3rd International Conference on, 8-10 April 2011. 278-280.
- Wang, S., Y. Gong, G. Chen, Q. Sun and F. Yang. 2013. Service vulnerability scanning based on service-oriented architecture in Web service environments. *Journal of Systems Architecture*, 59: 731-739.
- Weber, S., P. A. Karger and A. Paradkar. 2005. *A software flaw taxonomy: aiming tools at security*. In: SESS '05 Proceedings of the 2005 workshop on Software engineering for secure systems—building trustworthy applications, St. Louis, Missouri: ACM: 1-7.
- Wiesauer, A. and J. Sametinger. 2009. *A security design pattern taxonomy based on attack patterns: Findings of a systematic literature review*. ECRYPT 2009, Proceedings of the International Conference on Security and Cryptography, Milan, Italy, July 7-10, 2009, 387-

394.

- Xiaohui, K., W. Yan, X. Fei and L. Xiang. 2012. *A multi-dimension vulnerability analysis framework for large-scale distributed system*. In: Systems and Informatics (ICSAI), 2012 International Conference on, 19-20 May 2012. 843-848.
- Yan, W., H. Siy and R Gandhi. 2011. *Empirical results on the study of software vulnerabilities: NIER track*. In: Software Engineering (ICSE), 33rd International Conference on, 21-28 May 2011. 964-967.
- Yonglin, S., W. Yongjun, H. Xin, R. Zhanrui and L. Jie. 2011. *A new perspective of network vulnerability analysis using Network Security Gradient*. In: Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, 11-14 Dec. 2011. 159-163.
- Zeidanloo, H. R., M. J. Z. Shooshtari, P. V. Amoli, M. Safari and M. Zamani. 2010. *A taxonomy of Botnet detection techniques*. In: 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT); Chengdu: 2010, 158-162.
- Zhang, D., D. Liu, C. Csallner, D. Kung and Y. Lei. 2014. A distributed framework for demand-driven software vulnerability detection. *Journal of Systems and Software*, 87: 60-73.
- Zhongwen, Z. and D. Yingchun. 2012. *A New Method of Vulnerability Taxonomy Based on Information Security Attributes*. In: Computer and Information Technology (CIT), IEEE 12th International Conference on, 27-29 Oct. 2012. 739-741.