ارائهٔ یک روش محاسباتی به‌منظور کمی‌سازی میزان آسیب‌پذیری شبکه‌های رایانه‌ای بر اساس سیستم امتیازدهی آسیب‌پذیری متعارف

محمدحسین شرکت[1] | شهریار محمدی[2] | مونا جامی‌پور[3]

۱. دکتری مدیریت سیستم‌ها؛ گروه مدیریت فناوری اطلاعات؛ دانشگاه تهران؛ دانشکدهٔ 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 سیستم‌ها؛ گروه مدیریت فناوری اطلاعات؛ دانشکده مدیریت؛ دانشگاه تهران
mjamporazmay@yahoo.com

مقالهٔ پژوهشی

دریافت: ۱۳۹۱/۰۶/۱۴
پذیرش: ۱۳۹۲/۱۲/۱۸

دورهٔ ۲۹ شماره ۴
ص‌ص. ۱۱۰۷-۱۱۴۵

چکیده: افزایش تعداد آسیب‌پذیری‌ها و پیچیدگی آنها در حوزهٔ تبادل داده و اطلاعات، اهمیت مسئلهٔ کمی‌سازی آسیب‌پذیری‌ها را هم به جهت تعیین میزان آن و هم از نظر اولویت‌دهی و مدیریت منابع، بیش از پیش حائز اهمیت ساخته است. شبکه‌های رایانه‌ای به‌دلیل داشتن جایگاه پُراهمیت در زیرساخت ارتباطی و تبادل داده‌ها و اطلاعات همواره در معرض آسیب‌پذیری‌های متعددی قرار داشته‌اند و این مسئله لزوم محاسبهٔ کمی میزان آسیب‌پذیری‌ها را به‌منظور امکان دستیابی به شبکه‌هایی امن، بیش از پیش معطوف نظر محققان ساخته است. در این مقاله تلاش شده به‌منظور محاسبهٔ کمی آسیب‌پذیری‌های شبکه، یک روش توسعه‌یافته بر پایهٔ معماری امنیت ITU-TX- 805 و بر پایهٔ ویرایش دوم سیستم امتیازدهی آسیب‌پذیری متعارف (CVSS) پیشنهاد گردد. هدف روش پیشنهادی در این تحقیق، فراهم‌آوردن یک ساختار کمی‌سازی به‌منظور امکان شناسایی میزان آسیب‌پذیری‌ها و مدیریت مؤثر آنها می‌باشد.

کلیدواژه‌ها: آسیب‌پذیری؛ آسیب‌پذیری شبکه‌های رایانه‌ای؛ معماری امنیت ITU-TX- 805؛ کمی‌سازی آسیب‌پذیری‌ها؛ سیستم امتیازدهی آسیب‌پذیری متعارف (CVSS)

پژوهشنامهٔ پردازش و مدیریت اطلاعات
فصلنامه | علمی پژوهشی
شاپا (چاپی) ۸۲۲۳-۲۲۵۱
شاپا (الکترونیکی) ۸۲۳۱-۲۲۵۱
نمایه در LISA، ISC و Scopus
http://jipm.irandoc.ac.ir
پژوهشگاه علوم و فناوری اطلاعات ایران

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 به‌وجود آورد (Hansmann et al 2005). بر اساس تعریف «راماکریشنان» و «سکار» آسیب‌پذیری یکی از نقاط ضعف سیستم است که از آن می‌توان برای به‌خطر انداختن امنیت سیستم سوءاستفاده کرد (Ramakrishnan and Sekar1998). «بیشاپ» آسیب‌پذیری را به‌عنوان یکی از ویژگی‌های سیستم می‌داند که از یک‌سو به‌طور بالقوه باعث سوءاستفاده از سیستم می‌شود و از سوی دیگر می‌تواند خود نتیجهٔ یک یا چند حمله یا سوءاستفادهٔ 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 درجهٔ 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 مؤثرِ منابع در مواجهه با آسیب‌ها امری لازم و اساسی است.

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

نسبت به ارائهٔ یک روش کمی‌سازی در حوزهٔ محاسبه آسیب‌پذیری‌های شبکه‌های رایانه‌ای بر پایهٔ ویرایش دوم سیستم امتیازدهی آسیب پذیری متعارف[1] با عنوان NCVSS اقدام گردد. معماری امنیت ITU-TX-805 در مقایسه با سایر چارچوب‌ها و معماری‌های امنیتی جامع‌تر بوده و ضمن قابلیت به‌کارگیری برای کلیهٔ شبکه‌ها، یک نمای جامع و بالا به پایین از امنیت شبکه را برای اجزاء، سرویس‌ها و کاربردهای شبکه جهت شناسایی، پیشگیری و اصلاح آسیب‌پذیری‌ها فراهم می‌نماید (حاجیان و دیگران ۱۳۸۸).

این مقاله در ۵ بخش تنظیم شده‌است. پس از مقدمه، در بخش دوم به مطالعهٔ ادبیات موضوع و طبقه‌بندی آسیب‌پذیری‌ها پرداخته می‌شود. در بخش سوم، روش پیشنهادی برای محاسبهٔ کمی آسیب‌پذیری‌ها ارائه شده و بخش چهارم به آزمون روش پیشنهادی می‌پردازد. بخش پنجم شامل جمع‌بندی نتایج و نتیجه‌گیری است.

۲. مروری بر ادبیات موضوع

در مطالعهٔ علمیِ هر حوزهٔ جدید علمی وجود ساختار و یا چارچوبِ بررسی به‌عنوان پیش‌نیازی لازم و مهم برای مطالعهٔ 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 حوزهٔ آسیب‌پذیری معتقد است که تعریف چارچوب مؤثر می‌تواند زمینه‌ساز تعریف یک دسته‌بندی مناسب به‌منظور طبقه‌بندی آسیب‌پذیری‌ها گردیده و این طبقه‌بندی خود مبنایی برای مدیریت مؤثر آسیب‌پذیرها گردد(Krsul 1998). «لاف» ضمن بیان ضرورت ساخت‌یافته‌بودن، جامعیت، وضوح و کارآمدی در هر نوع ساختار مدیریت آسیب‌پذیرها، معتقد است که یک ساختار با فراهم‌کردن مفاهیم مشترک در دسته‌بندی آسیب‌پذیری‌ها، راه ساخت‌یافته‌ای را جهت مشاهده، تحلیل و ارزیابی کمی و کیفی آسیب‌پذیری‌ها فراهم می‌نماید(Lough 2001).

«بیشاپ» معتقد است که اولین مرحله برای مدیریت مؤثر آسیب‌پذیری‌ها، فهم آسیب‌پذیری‌ها بر اساس دسته‌بندی آنها بر مبنای مشخصاتشان در رده‌بندی است، چرا که این کار تعداد زیادی از آسیب‌پذیری‌ها را بر طبق یک گروه‌بندی، قابل فهم می‌سازد (Bishop 2003). بنا به اعتقاد «بیسبی» و «هالینگورث» یکی از اهداف تولید رده‌بندی‌های

1. Common Vulnerability Scoring System: CVSS

آسیب‌پذیری، توسعهٔ ابزارهای خودکار جهت انجام ارزیابی‌های کمی در حوزهٔ امنیت است (Bisbey & Hollingworth 1978).

تاکنون رده‌بندی‌های متعددی در حوزه آسیب‌پذیری ارائه شده‌است. جدول شماره ۱ خلاصهٔ مهم‌ترین رده‌بندی‌های انجام‌شده در حوزهٔ آسیب‌پذیری و مشخصات کلیدی هر یک را نمایش می‌دهد. شاید بتوان گفت که اولین دسته‌بندی در حوزه آسیب‌پذیری 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 آسیب‌پذیری‌های نرم‌افزاری، به‌خصوص سیستم‌های عامل نمود (Ammala 2004).

جدول ۱. خلاصهٔ مهم‌ترین رده‌بندی‌های انجام‌شده در حوزهٔ آسیب‌پذیری

ردیف	محقق/ محققان	مبنای رده‌بندی	تمرکز موضوعی	مشخصه
۱	Abbott et al, 1976	اشکالات و آسیب‌پذیری‌های زمان برنامه‌نویسی و تولید کد برنامه	سیستم‌عامل‌ها	تک‌لایه
۲	Bisbey et al, 1978	خطاهای حفاظتی در فرایند استفاده	سیستم‌عامل‌ها	تک‌لایه
۳	Ristenbatt, 1988	طراحی شبکه و ویژگی‌های در معرض آسیب	شبکه‌ها	تک‌لایه
۴	Landwehr et al, 1994	پیدایش، مکان رخنه و زمان ایجاد رخنه	نرم‌افزارها	تک‌لایه
۵	Aslam, 1995	اشکالات و آسیب‌پذیری‌های زمان برنامه‌نویسی و تولید کد برنامه	سیستم‌عامل UNIX	تک‌لایه
۶	Bishop, 1995	اشکالات و آسیب‌پذیری‌های زمان برنامه‌نویسی و تولید کد برنامه	نرم‌افزارها	تک‌لایه

ردیف	محقق/ محققان	مبنای رده‌بندی	تمرکز موضوعی	مشخصه
۷	Du, 1997	انواع حملات و آسیب‌پذیری‌های دیواره‌های آتش	شبکه‌ها	تک‌لایه
۸	Bishop, 1999	طبیعت، زمان رخداد، سوءاستفاده، اثر، حداقل تعداد اجزاء آسیب‌پذیر، منبع شناسایی	عمومی	تک‌لایه
۹	Kamara, 2003	انواع حملات و آسیب پذیری‌های دیواره‌های آتش	دیواره‌های آتش	تک‌لایه
۱۰	Pothamsetty et al, 2004	رخنه‌های موجود در پروتکل‌های نرم‌افزاری	پروتکل	تک‌لایه
۱۱	Weber, et al, 2005	چگونگی پیدایش و علل ایجاد رخنه	نرم افزارها	تک‌لایه
۱۲	Hamed et al, 2006	ناسازگاری سیاست امنیتی	شبکه‌ها	تک‌لایه
۱۳	Asosheh et al, 2008	خطرات ناشی از انکار سرویس توزیع‌شده (DDoS)	شبکه‌ها	تک‌لایه
۱۴	Wiesauer et al, 2009	الگوی حملات	نرم‌افزارها	تک‌لایه
۱۵	Ryoo et al, 2009	چگونگی پیدایش و علل ایجاد رخنه	شبکه‌های بی‌سیم	سلسله مراتبی و چندبعدی
۱۶	Zeidanloo et al, 2010	honeynetها و IDS	Botnet ها	تک‌لایه
۱۷	Alvi and Zulkernine, 2011	رده‌بندی آسیب‌پذیری‌ها بر اساس فازهای دورهٔ عمر نرم‌افزار	نرم‌افزار	---

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 برنامه نویسی C	نرم‌افزار	---
۲۰	Kuhn, 2011	رده‌بندی آسیب‌پذیری‌ها بر اساس سیاست کنترل دسترسی و شناسایی خطاهای پیکره‌بندی	تست کلاس‌های خاص معرفی‌شده	چندلایه‌ای و چندبعدی
۲۱	Hunt and Slay, 2011	طبقه‌بندی آسیب‌پذیری‌ها به‌منظور دست‌یابی به فناوری‌های جدید برای مقابله با انواع مکانیزم‌های جدید دفاعی	سیستم‌های توسعه‌یافته مانند محاسبات ابری، بدافزارهای سه‌بعدی و VOIPها	---
۲۲	Yan et al., 2011	دسته‌بندی آسیب‌پذیری‌ها با استفاده از آزمایش‌های تجربی به‌منظور ارزیابی کارایی الگوهای معنایی	نرم افزار	---
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 رده‌بندی	تمرکز موضوعی	مشخصه
۲۵	Gallon and Bascou, 2011	۱- استفاده از چارچوب CVSS به‌منظور نمره‌دهی عددی به آسیب‌پذیری‌های ثبت‌شده در پایگاه‌های داده CVE، ۲- ایجاد ارتباط بین گراف‌های حمله با چارچوب CVSS به‌منظور ارزیابی اثر حمله‌ها بر میزبان شبکه هدف	شبکه‌های رایانه‌ای	---
۲۶	Vijayakumar and Muthuchelvi, 2011	استفاده از XDOS و TCP/IP برای کشف اتوماتیک آسیب‌پذیری‌های Zombie	نرم‌افزار	---
۲۷	Shahriar and Zulkernine, 2011	۱- طبقه‌بندی آسیب‌پذیری‌ها با توجه به ویژگی‌های عمومی در حملات آنلاین ۲- طبقه‌بندی آسیب‌پذیری‌ها بر اساس تفاوت ویژگی‌های برنامه در حال اجرا با ویژگی‌های ثبت‌شده	برنامه‌های نرم‌افزاری	---
۲۸	Perla et al., 2011	طبقه‌بندی آسیب‌پذیری‌ها بر اساس خطاهای منطقی، شرایط رقابتی و نتایج عملیات منطقی	سیستم‌عامل	---
۲۹	Holm et al., 2012	استفاده از چارچوب CVSS به‌منظور تعیین سطح آسیب‌پذیری سیستم‌ها	شبکه‌های کامپیوتری	---
۳۰	Zhongwen and Yingchun, 2012	رده‌بندی آسیب‌پذیری‌ها بر پایهٔ پنج ویژگی امنیت اطلاعات شامل یکپارچگی، دسترس‌پذیری، 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 چرخهٔ عمر نرم‌افزار	سیستم‌های توزیع‌شده در مقیاس وسیع	چندلایه‌ای و چندبعدی
۳۲	Hudic et al., 2012	استفاده از مکانیزم‌های تست نفوذ به‌منظور طبقه‌بندی آسیب‌پذیری‌های پایگاه داده، سیستم‌های رایانه‌ای و شبکه‌ها	پایگاه داده، سیستم‌های رایانه‌ای و شبکه	---
۳۳	JunGang et al., 2012	تشخیص هویت میزبان‌ها به‌منظور 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	ارائهٔ متدهای تحلیل آسیب‌پذیری در زمینهٔ امنیت شبکه به‌منظور تشخیص طبقه‌بندی مناسب برای آسیب‌پذیری‌ها	شبکه‌های ad hoc، شبکه‌های 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 ارث‌بری‌شده از لایه‌های پایین به‌منظور ارائهٔ دسته‌بندی مناسب از آسیب‌پذیری	زمان و مکان حمله‌ها در سیستم‌های رایانه‌ای	سلسله‌مراتبی
۳۷	Bhattacharya and Ghosh, 2012	دسته‌بندی آسیب‌پذیری‌ها با استفاده از گراف وابستگی به‌منظور شناسایی حملات و آسیب‌پذیری‌های به‌وجود آمده	شبکه	---

ردیف	محقق/ محققان	مبنای رده‌بندی	تمرکز موضوعی	مشخصه
۳۸	Njogu et al., 2013	طبقه‌بندی آسیب‌پذیری‌ها 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 به‌جای شمردن تمام آسیب‌ها، به ارزیابی آسیب‌هایی می‌پردازد که ممکن است تخریب زیادی روی امنیت شبکه بگذارند	شبکه‌های رایانه‌ای	---
۴۰	Ben-Porat, 2013	استفاده از Closed-Hash برای ارزیابی ساختار داده به‌منظور تعیین میزان آسیب‌پذیری	شبکه‌های رایانه‌ای	---
۴۱	Marrone et al., 2013	ارائه زبان مدل‌سازی برای تحلیل آسیب‌پذیری‌ها در برنامه‌های کاربردی به‌منظور حفاظت از ساختار حیاتی برنامه‌ها	نرم‌افزار	---
۴۲	Kakareka, 2013	استفاده از XML برای ارزیابی آسیب‌پذیری سیستم	سیستم‌های رایانه‌ای	---
۴۳	Wang et al., 2013	استفاده از الگوی پیمایش آسیب‌پذیری سرویس بر پایه معماری SOA در محیط وب سرویس	محیط‌های وب سرویس	سلسله‌مراتبی
۴۴	Zhang et al., 2014	استفاده از سیستم امنیتی تا بتوان با تشخیص آسیب‌پذیری، آن را به همه کلاینت‌ها ارسال نمود	نرم‌افزار	---

با مروری بر مطالعات انجام‌شده و موارد مندرج در جدول شماره ۱ می‌توان به این نتیجه رسید که در دسته‌بندی‌های ارائه‌شده معیارها و فاکتورهای متفاوتی برای دسته‌بندی و رده‌بندی آسیب‌پذیری‌ها استفاده شده است. این معیارها عبارتند از:

- ◇ دسته‌بندی آسیب‌پذیری‌ها با توجه به روشی که از آنها سوءاستفاده می‌شود؛
- ◇ دسته‌بندی به مؤلفه‌های نرم‌افزاری و سخت‌افزاری و رابطه‌ای که باعث بروز آسیب‌پذیری می‌شو؛
- ◇ دسته‌بندی بر اساس ماهیت آسیب‌پذیری و دلایل ایجاد آن؛
- ◇ دسته‌بندی آسیب‌پذیری‌ها بر اساس زمان وقوع آنها؛ و
- ◇ دسته‌بندی آسیب‌پذیری‌ها بر اساس دامنهٔ آن.

با توجه به اینکه در موضوع امنیت شبکه هدف از بررسی و تحلیل آسیب‌پذیری‌ها، شناسایی و کشف حمله قبل از وقوع آن بر اساس میزان آسیب‌پذیری هر یک از مؤلفه‌های امنیتی به‌منظور اتخاذ تدابیر لازم در جهت مواجهه با آسیب‌پذیری است، آنها باید به‌گونه‌ای بررسی و رده‌بندی شوند که امکان محاسبهٔ میزان آسیب‌پذیری‌ها را با هدف امکان تعیین نقش و اثر آسیب‌پذیری‌های شبکه فراهم آورند (امیدیان و دیگران ۱۳۸۸). بر این اساس یکی از نواقص قابل مشاهده در فعالیت‌های انجام شدهٔ قبلی فقدان یک ساختار کمی‌سازی در چارچوب‌های بررسی و طبقه‌بندی آسیب‌پذیری‌هاست.

تاکنون مطالعات محدودی به‌منظور ارائهٔ روش‌های ارزیابی و محاسبهٔ کمی آسیب‌پذیری‌ها انجام گردیده است. «جورج» و «وامانو» چارچوب عملی عمومی را جهت ارزیابی کمی آسیب‌پذیری سیستم‌ها ارائه نموده‌اند (gheorghe and Vamanu 2004). در این چارچوب، میزان آسیب‌پذیری سیستم به شکل کمی، و به‌صورت عددی بین ۰ تا ۱۰۰ اندازه‌گیری می‌شود. الحزمی و مالائیا معیاری با نام چگالی آسیب‌پذیری را به‌عنوان معیاری جهت ارزیابی میزان آسیب‌پذیری سیستم‌ها و امکان پیش‌بینی نرخ کشف آسیب‌پذیری‌ها در آینده معرفی نموده‌اند (Alhazmi and Malaiya 2005). امامی و جعفریان نیز به ارائهٔ چارچوبی برای محاسبهٔ درجهٔ آسیب‌پذیری سیستم‌های مدیریت پایگاه داده‌های متن باز رایج پرداخته‌اند (۲۰۰۹). در این مطالعه، روشی برای ارزیابی میزان آسیب‌پذیری سیستم‌های هم‌نوع با استفاده از تعداد آسیب‌پذیری‌ها، تعداد نسخ رایج و

میزان محبوبیت آنها معرفی شده و چارچوب پیشنهادی برای محاسبهٔ کمی آسیب‌پذیری پایگاه‌های داده متن باز Firebird, Ingres, PostgreSQL, MySQL, مورد استفاده قرار گرفته است (امامی و دیگران ۱۳۸۸). به‌منظور ایمن‌سازی و دستیابی به شبکه‌های امن نیز رویکردهای مختلفی ارائه گردیده که در جدول شماره ۲ به‌صورت خلاصه به اهم موارد مندرج در تحقیقات سال‌های اخیر پرداخته شده است.

جدول ۲. رویکردهای متأخر در ایمن‌سازی و دست‌یابی به شبکه‌های امن

سال- محقق	بررسی صورت‌گرفته	تمرکز موضوعی
(Taheri et al. 2010)	مسیریابی MultiPath برای تشخیص و محافظت از حملات کرم‌ها	شبکه‌های بی‌سیم و موردی
(Nehinbe 2011)	مرور راهنمایی‌های موجود برای افزایش نظارت بر نفوذ به سیستم	سیستم‌های رایانه‌ای
(Yonglin et al. 2011)	ایجاد گراف حمله به‌منظور تشخیص حملات غیرمستقیم	شبکه‌های رایانه‌ای
(Asman et al. 2011)	شبیه‌سازی عامل‌گرا با توجه به جریان بسته‌ها و بررسی رفتار آنها به‌منظور شناسایی جریان‌های مخرب	سیستم‌های رایانه‌ای، مسیریاب‌ها و سرورها
(Hudic et al. 2012)	طبقه‌بندی مناسب برای پوشش فرایند Penetration Test	پایگاه داده، سیستم‌های رایانه‌ای
(Kundu et al. 2012)	استفاده از گراف به‌منظور تحلیل آسیب‌های امنیتی موجود و تشخیص میزان امن‌بودن سیستم	شبکه‌های رایانه‌ای
(Junshun et al. 2012)	تشخیص خطاها و محل رویداد آنها با استفاده از ابزار SMT به‌منظور چک‌کردن صحت داده‌ها	شبکه‌های رایانه‌ای
Saxena and Hote) (2013	استفاده از تئوری Rough Set به‌منظور ترکیب فاکتورهای حمله و تشخیص احتمال وقوع حمله	سیستم‌های رایانه‌ای LAN
(Jiang et al. 2013)	استراتژی ارزیابی و آگاهی از حملات به‌صورت عامل‌گرا	شبکه‌های رایانه‌ای

سال- محقق	بررسی صورت‌گرفته	تمرکز موضوعی
Hernandez-Ardieta) (et al. 2013	طبقه‌بندی حمله‌های صورت‌گرفته در امضای دیجیتال به‌صورتی که فاز تولید و تصدیق امضای دیجیتال را پوشش می‌دهد	امضای دیجیتال
(Corona et al. 2013)	طبقه‌بندی کلی تکنیک‌های حمله به‌منظور داشتن تشخیص نفوذ مناسب	سیستم‌های رایانه‌ای
Avramescu et al.) (2013	استفاده از Penetration Test برای تشخیص حملات	شبکه‌های رایانه‌ای، برنامه‌های تحت وب، پایگاه داده SQL

۳. روش پیشنهادی

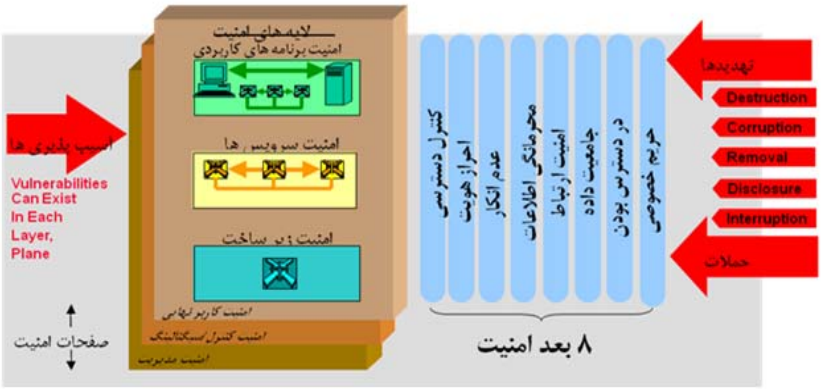
بر اساس آنچه که در بخش قبل اشاره گردید، در این بخش تلاش می‌شود نسبت به ارائهٔ یک روش محاسباتی به‌منظور محاسبهٔ کمی میزان آسیب‌پذیری‌های شبکه‌های رایانه‌ای اقدام گردد. همان‌گونه که در مقدمه اشاره شد، نخست لازم است ساختار و چارچوب مورد نظر جهت ارائهٔ روش کمی‌سازی تعریف گردیده و بر اساس آن نسبت به ارائهٔ روش محاسباتی اقدام شود. با توجه به هدف تحقیق، ساختار و چارچوب مورد استفاده باید مشخص نماید که چه فعالیت‌هایی در ساختار شبکه در معرض آسیب‌پذیری قرار دارند و باید محافظت شوند تا بر اساس آن بتوان نسبت به محاسبهٔ میزان آسیب‌پذیری‌ها اقدام نمود.

برای تعیین این فعالیت‌ها 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 می‌دهد. دلایل استفاده از این معماری در روش پیشنهادی را می‌توان به‌طور خلاصه چنین بیان کرد:

۱. معماری امنیت ITU-TX-805 به‌گونه‌ای طراحی‌شده که برای کلیهٔ شبکه‌ها و کاربردها قابل به‌کارگیری بوده و نگرانی‌های امنیتی مربوط به مدیریت، کنترل و استفاده از زیرساخت، سرویس‌ها و کاربردهای شبکه را مد نظر قرار می‌دهد؛ و

۲. نمای جامع و بالا به پایینی از امنیت شبکه را برای عناصر، سرویس‌ها و کاربردهای شبکه فراهم می‌کند (مک‌گی[1] و دیگران ۲۰۰۴).

ساختار معماری ITU-TX-805 سه مؤلفهٔ ابعاد یا جنبه‌های امنیتی، لایه‌های امنیتی، و سطوح امنیتی را شامل است. در این تحقیق به‌منظور تعیین فعالیت‌هایی که در معرض آسیب‌پذیری در ساختار شبکه می‌باشند، بر روی ابعاد و یا جنبه‌های امنیتی معماری امنیت اطلاعات تمرکز شده‌است.



شکل ۱. ساختار معماری امنیت ITU-TX- 805 (مک‌گی و دیگران ۲۰۰٤)

ابعاد امنیتی، مجموعه‌ای از اقدامات امنیتی است که جهت مشخص‌کردن جنبهٔ خاصی از امنیت شبکه طراحی شده است. در این معماری، هشت مجموعهٔ مشخص‌شده در بُعد امنیت شامل کنترل دسترسی، احراز هویت، عدم انکار، محرمانگی داده‌ها، امنیت ارتباطات، تمامیت داده، قابلیت دسترسی و حریم خصوصی حفاظت در برابر کلیه تهدیدهای امنیتی اصلی فراهم می‌آید. در این معماری جهت فراهم‌شدن راه‌حل امنیت کامل، ابعاد امنیتی را بایستی بتوان برای ساختار سلسله‌مراتبی تجهیزات و اجزاء شبکه که تحت عنوان لایه‌های امنیت نامگذاری می‌شود، به‌کار برد. بر این اساس سه لایهٔ امنیتیِ زیرساخت، سرویس و کاربردی در این معماری تعریف شده است. هر لایه بر روی لایهٔ

1. McGee

دیگر ساخته‌شده تا یک راه‌حل جامع فراهم شود. در این شرایط لایهٔ زیرساخت، لایهٔ سرویس و لایهٔ 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 به‌وسیلهٔ ابعاد امنیتی محافظت می‌شوند. در این معماری سه سطح امنیتی برای ارائهٔ سه گروه از فعالیت‌هایی که در شبکه اتفاق می‌افتد، تحت عنوان سطح مدیریت، سطح کنترل و سطح کاربر نهایی تعریف شده است. اِعمال ۸ 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 رخنهٔ امنیتی یا یک آسیب‌پذیری را موشکافانه ارزیابی نماید.

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

نکتهٔ قابل توجه دیگر در انتخاب جنبه‌های امنیتی معماری امنیت ITU-TX-805 به‌عنوان ساختار تعیین فعالیت‌های در معرض آسیب پذیری در ارائهٔ روش کمی‌سازی آسیب پذیری‌ها در این تحقیق، ماهیت چندوجهی رخداد هر آسیب‌پذیری است. به‌عبارت 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 به‌صورت ترکیبی بوده و به‌عبارتی با در کنار هم قرارگرفتن دو سرویس خاص و یا گاهی یک سرویس در کنار یکی از عناصر زیرساخت شبکه یا کاربرد خاص ایجاد مشکل می‌کند. به‌منظور محاسبهٔ کمی آسیب‌پذیری‌های شبکه در بُعد جنبه‌های امنیتی برای ساختار مورد استفاده در این تحقیق، از سیستم امتیازدهی آسیب پذیری متعارف (CVSS) که در سال ۲۰۰۷ توسط مجمع واکنش به وقایع و گروه‌های امنیتی (FIRST) ارائه گردیده، استفاده شده است.

سیستم امتیاز دهی آسیب پذیری 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 به‌نوبهٔ خود شامل مجموعه‌ای از زیرمعیارهای دیگر می‌باشد. معیارهای پایه‌ای، ویژگی‌های اصلی و پایه‌ای یک آسیب‌پذیری هستند که در طول زمان ثابت بوده و به محیط کاربر بستگی ندارند. در مقابل، معیارهای موقتی با گذشت زمان تغییر می‌کنند، ولی بین محیط‌های کاربری مختلف یکسان هستند. معیارهای محیطی نیز به یک محیط خاص کاربری مربوط بوده و منحصر به آن محیط می‌باشند (Mell et al 2006).

از ویژگی‌های روش CVSS سادگی و سهولت درک آن است. در این روش، وقتی که به معیارهای پایه‌ای مقادیر مناسبی اختصاص داده شود، معادلهٔ پایه‌ای، مقداری بین ۰ تا ۱۰ خواهد گرفت. استفاده از معیارهای موقتی و محیطی اختیاری است، ولی می‌توان با تخصیص مقادیر مناسب به این معیارها امتیاز پایه را بالایش کرد. استفاده از معیارهای موقتی و محیطی میزان ریسک ناشی از آسیب‌پذیری را با دقت بیشتری منعکس می‌سازد، اما استفاده از این معیار ها الزامی نیست و با توجه به هدف، ممکن است استفاده از امتیاز پایه کافی باشد (همان).

تاکنون مطالعات متعددی به‌منظور متناسب‌سازی مدل پایه CVSS برای سازمان‌ها و محاسبهٔ آسیب‌پذیری‌ها برای مقاصد مختلف و همچنین افزایش کارآیی مدل پایه انجام شده است. به‌عنوان نمونه می‌توان به مطالعات زیر اشاره کرد: تعیین نقاط کارآمدی و ناکارآمدی مدل CVSS و متناسب‌سازی آن (Scarfone et al 2009; Mell et al 2007)؛ لزوم بومی‌سازی مدل پایهٔ CVSS در سازمان‌های مختلف و اهمیت بومی‌سازی مدل به‌منظور بهره‌مندی از مزایای آن (Fruhwirth and Mannisto 2009)؛ بررسی اثرات معیارهای محیطی بر کارآمدی مدل CVSS و ارائهٔ راهکارهایی به‌منظور تأثیردهی دقیق معیارهای محیطی به‌عنوان عامل اصلی در بومی‌سازی مدل (Gallon 2010)؛ و اهمیت معیارهای محیطی در متناسب‌سازی مدل پایه CVSS و نقش معیار توزیع هدف به‌عنوان یک معیار متناسب‌کننده در تأثیردهی شرایط محیطی سازمان‌ها در فرایند محاسبهٔ مؤثر این روش (Harada et al 2010).

«هامب» و «فرانکریا» نیز به ارائهٔ مدلی به‌منظور پیش‌بینی میزان احتمال رخداد آسیب‌پذیری و ریسک حاصل از آن در سازمان‌ها بر اساس مدل CVSS پرداخته‌اند (Houmb and Franqueira 2009). در این تحقیق با ارائهٔ دو شاخص تکرار سوءاستفاده و اثر

سوءاستفاده از آسیب‌پذیری‌ها به پیش‌بینی آسیب‌پذیری‌ها بر اساس فرایند «مارکوف»[1] 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 مقایسهٔ 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[2] (NCVSS) نامیده شده است. جدول شماره ۳ به مقایسهٔ مؤلفه‌های جنبه‌های امنیتی شبکه معماری امنیت TU-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 زمینهٔ مؤلفهٔ 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 به‌صورت 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

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

جدول ٤. معیارهای پایه مؤلفه‌های روش NCVSS و تطابق آن با مؤلفه‌های ساختار جنبه‌های امنیتی معماری امنیت ITU-TX- 805

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

بر اساس موارد اشاره‌شده، معیارهای پایه‌ای و مشخصه‌های آن بر پایهٔ مدل CVSS به‌منظور استفاده در موضوع این مقاله در قالب روش NCVSS به‌صورت جدول شماره ۵ پیشنهاد شده است. همان‌گونه که از این جدول برمی‌آید، در مقایسهٔ مدل CVSS با روش

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

جدول ۵. معیارهای پایه در روش NCVSS

معیار	مشخصه	مقدار کمی	توضیح
بردار دسترسی	شبکه LAN داخلی	۰/۳۹۵	در آسیب‌پذیری که فقط با دسترسی محلی قابل بهره‌برداری است، حمله‌کننده به دسترسی فیزیکی به سیستم آسیب‌پذیر یا یک حساب محلی نیاز دارد.
	بی‌سیم W-LAN	۰/۴۶۴	حمله‌کننده باید در دامنه شبکه بی‌سیم قرار داشته باشد.
	شبکه اینترنت	۱	در آسیب‌پذیری قابل بهره‌برداری از راه شبکه اینترنت، حمله‌کننده نیاز به دسترسی به شبکه LAN و یا قرارگرفتن در دامنه شبکه ندارد.
پیچیدگی دسترسی	زیاد (H)	۰/۳۵	شرایط دسترسی لازم است. در این موارد حمله‌کننده باید دارای مهارت‌های سطح بالا باشد، اطلاعات مورد نیاز جهت فعالیت به‌صورت دستی قابل دستیابی نبوده و حمله‌کننده باید نرم افزارهای تخصصی را در اختیار داشته باشد.
	متوسط (M)	۰/۶۱	شرایط دسترسی تا حدی تخصصی هستند. در این موارد حمله‌کننده باید دارای مهارت بوده و اطلاعاتی را از درون شبکه جمع‌آوری نماید تا بر اساس آن عمل کند. شبکه فاقد تنظیمات پیش‌فرض است.
	کم (L)	۰/۷۱	شرایط دسترسی تخصصی وجود ندارد. در این حالت نیاز به مهارت کمی وجود دارد و به‌صورت دستی و بدون استفاده از نرم‌افزارهای خاص نفوذ به شبکه امکان‌پذیر باشد و به اطلاعات اضافی جهت بهره‌برداری از شبکه نیازی نیست.

معیار	مشخصه	مقدار کمی	توضیح
تصدیق اصالت	متعدد (M)	۰/۴۵	حمله‌کننده برای بهره‌برداری از آسیب‌پذیری 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 بهره‌برداری از آسیب‌پذیری نیاز است.
	هیچ (N)	۰/۷۴	برای بهره‌برداری از آسیب‌پذیری به تصدیق اصالت نیاز نیست
تصدیق فعالیت	متعدد (M)	۰/۴۵	راه‌های متعددی برای اثبات فعالیت‌های انجام‌شده در سیستم وجود دارد
	واحد (S)	۰/۵۶	یک راه برای تصدیق فعالیت‌های انجام‌شده وجود دارد
	هیچ (N)	۰/۷۰۴	هیچ راهی به‌منظور 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 فایل‌های سیستم امکان‌پذیر است، ولی حمله‌کننده کنترلی روی چیزی که به‌دست می‌آورد، ندارد یا حوزه زیان، محدوده شده است به‌عنوان مثال، می‌توان به آسیب‌پذیری که فقط می‌تواند جداول خاصی از پایگاه داده را افشاء سازد، اشاره کرد.
	کامل (C)	۰/۶۶	همه فایل‌های سیستم افشاء شده‌اند و حمله‌کننده می‌تواند همه داده‌های سیستم را بخواند.
تأثیر بر امنیت ارتباطات	متعدد (M)	۰/۴۵	لایه‌های 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 امن‌سازی ارتباطات وجود ندارد.

معیار	مشخصه	مقدار کمی	توضیح
تأثیر جامعیت	هیچ (N)	۰	تأثیری روی جامعیت اطلاعات ندارد (هیچ‌گونه تغییری در اطلاعات و یا فایل‌های موجود بر روی سیستم فعال در شبکه ایجاد نمی‌شود)
	ناقص (P)	۰/۲۷۵	تغییر برخی فایل‌ها یا اطلاعات ممکن است، ولی حمله‌کننده کنترل روی آنچه می‌تواند تغییر داده شود، ندارد یا حوزه‌ای که حمله‌کننده می‌تواند آن را تحت تأثیر قرار دهد، محدود است.
	کامل (C)	۰/۶۶	حمله‌کننده می‌تواند هر فایلی را تغییر دهد.
در دسترس‌پذیری	هیچ (N)	۰	تأثیری بر دسترسی‌پذیری سیستم ندارد.
	ناقص (P)	۰/۲۷۵	در دسترس کاربران مجاز وقفه‌هایی ایجاد نموده و یا کارایی آنها را کاهش می‌دهد.
	کامل (C)	۰/۶۶	بر اثر حمله، دسترسی سایرین به شبکه قطع می‌شود.

جدول ٦. معیارهای موقتی در روش NCVSS

معیار	مشخصه	مقدار کمی	توضیح
قابلیت بهره‌برداری	اثبات‌نشده (U)	۰/۸۵	نرم‌افزار یا ابزاری وجود ندارد و یا وجود آن در حد تئوری است.
	اثبات مفهوم (POC)	۰/۹	کدها یا تکنیک‌ها در همه موقعیت‌ها عملی نیست و ممکن است به تغییرات اساسی توسط حمله‌کننده نیاز داشته باشد.
	در حال کار (F)	۰/۹۵	ابزارها و نرم‌افزارهایی در دسترس است و در بسیاری از موقعیت‌هایی که آسیب‌پذیری وجود دارد، قابل استفاده و کاربری است.
	زیاد (H)	۱	ابزارها و نرم‌افزارهای گسترده و فراگیر به‌همراه جزئیات آنها در دسترس همه قرار دارد و استفاده از آن ساده و پُرکاربرد است.
	تعریف‌نشده (ND)	۱	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تأثیری نخواهد گذاشت.

معیار	مشخصه	مقدار کمی	توضیح
سطح ترمیم	ترمیم آسیب‌پذیری رسمی (OF)	۰/۸۷	سازمان، یک راه‌حل رسمی و تعریف‌شده دارد.
	ترمیم آسیب‌پذیری موقتی (TF)	۰/۹	سازمان، نسبت به تأمین یک راه‌حل موقتی اقدام نماید.
	دور زدن آسیب‌پذیری (W)	۰/۹۵	سازمان، نیازمند صرف وقت برای تعیین یک راه‌حل احتمالی جهت حل موضوع است، اما مسئله قابل حل می‌باشد.
	غیرقابل دسترس(U)	۱	راه‌حلی در دسترس نیست یا به‌کاربردن آن غیرممکن است.
	تعریف‌نشده (ND)	۱	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تأثیری نخواهدگذاشت.
اطمینان از گزارش	تأییدنشده (UN)	۰/۹	فقط یک منبع تأییدنشده آسیب‌پذیری را گزارش کرده است یا چندین گزارش متناقض وجود دارد که این گزارشات نیز اعتبار زیادی ندارند.
	اثبات‌نشده (UR)	۰/۹۵	چندین منبع غیررسمی مانند سازمان‌های امنیتی و تحقیقاتی گزارشاتی داده‌اند و ممکن است بین جزئیات فنی این گزارش‌ها تناقض وجود داشته باشد.
	تأییدشده (C)	۱	آسیب‌پذیری توسط مراجع ذیصلاح تأیید شده است.
	تعریف‌نشده (ND)	۱	با تخصیص این مقدار به معیار در محاسبهٔ امتیاز نهایی تأثیری نخواهد گذاشت.

به‌منظور کمی‌سازی نتایج و امتیازدهی به آسیب‌پذیری‌ها نیز معادلات پایهٔ مدل CVSS در قالب روش NCVSS مورد بازنگری قرار گرفته‌است. بر این اساس دو معیار تصدیق فعالیت و تأثیر بر امنیت ارتباطات به ساختار محاسبهٔ مدل CVSS اضافه گردیده است. همچنین در روش NCVSS معادلهٔ 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 می‌دهد.

مقدار امتیاز پایه $= \textbf{round to one decimal}\ (((0.6 * I) + (0.4 * E) - 1.5) * F$

$I = 10.41 * \left(1 - \left(1 - \right.\right.$ (تأثیر بر جامعیت $- 1) * \left(1 -\right.$ (تأثیر بر محرمانگی $- 1) * \left(1 -\right.$ دسترس‌پذیری$\left.\left.\right)\right)$

$E = 20 *$ امنیت ارتباطات * تصدیق فعالیت * تصدیق اصالت * پیچیدگی دسترسی * بردار دسترسی

$F =$ اگر $I = 0 \xrightarrow{\text{آنگاه}} F = 0$ در غیر اینصورت $F = 1.176$

مقدار امتیاز موقتی $= \textbf{round to one decimal}$ (قابلیت بهره‌برداری * مقدار امتیاز پایه * اطمینان از گزارش * سطح ترمیم)

مقدار امتیاز محیطی $= \textbf{round to one decimal}\ ((AT + (10 - AT)$ * (خسارت بالقوه * توزیع هدف)

$AB = ((0.6 * AI) + (0.4 * AI) - 1.5) * F$

$AT = AB *$ (اطمینان از گزارش * سطح ترمیم * قابلیت بهره‌برداری)

$AI = \min(10, 10.41 + (1 -$ تأثیر بر جامعیت $- 1)) *$ (نیازهای امنیتی * تأثیر بر محرمانگی $- 1) *$ (نیازهای امنیتی * دسترس‌پذیری $- 1) *$ (نیازهای امنیتی)

شکل ۲. معادلات پایه، موقتی و محیطی در روش پیشنهادی NCVSS

٤. روش تحقیق

٤-١. چارچوب نظری تحقیق

این تحقیق بر اساس هدف، از نوع تحقیقات کاربردی است، چرا که به توسعهٔ دانش در حیطهٔ ارزیابی کمی آسیب‌پذیری‌های شبکه می‌پردازد. همچنین، بر اساس چگونگی به‌دست آوردن داده‌های مورد نیاز، این تحقیق از نوع تحقیقات پیمایشی محسوب می‌گردد. چارچوب نظری پژوهش در جدول شماره ۷ ارائه شده است. متناسب با چارچوب نظری تحقیق، پرسشنامهٔ پژوهش طراحی و در بین جامعهٔ آماری توزیع گردیده و با تجزیه و تحلیل اطلاعات به‌دست آمده چارچوب نظریِ پیشنهادی به آزمون گذاشته شده است. برای تحلیل داده‌ها نیز تحلیل عاملی (تحلیل مؤلفه‌های اصلی و چرخش واریماکس) به‌کار رفته است.

جدول ۷. معیارهای محیطی در روش NCVSS

معیار	مشخصه	مقدار کمی	توضیح
میزان خسارت بالقوه	هیچ (N)	۰	امکان وارد آمدن خسارت و یا کاهش بازده و کارآیی وجود ندارد.
	کم (L)	۰/۱	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی کمی دارد یا روی کارآیی یا بازدهی تأثیر کمی می‌گذارد.
	کم ـ متوسط (LM)	۰/۳	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی متوسط دارد یا روی کارآیی یا بازدهی تأثیر متوسط دارد.
	متوسط ـ زیاد (MH)	۰/۴	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی مهمی دارد یا روی کارآیی یا بازدهی تأثیر مهمی می‌گذارد.
	زیاد (H)	۰/۵	بهره‌برداری موفق از آسیب‌پذیری خسارت فیزیکی یا مالی فاجعه‌باری دارد یا روی کارآیی یا بازدهی تأثیر فاجعه‌بار می‌گذارد.
	تعریف‌نشده (ND)	۰	با تخصیص این مقدار به معیار، این معیار در محاسبهٔ امتیاز نهایی تأثیری نخواهد گذاشت.
توزیع هدف	هیچ (N)	۰	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)	۰/۲۵	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)	۰/۷۵	اهداف در یک مقیاس متوسط در داخل محیط وجود دارند. بین ۷۵ الی ۲۶ درصد کل محیط در معرض ریسک قرار دارد.
	زیاد (H)	۱	اهداف در یک مقیاس قابل توجه در داخل محیط وجود دارند. بین ۱۰۰ الی ۷۶ درصد کل محیط در معرض ریسک قرار دارد.
	تعریف‌نشده (ND)	۱	با تخصیص این مقدار به معیار، این معیار روی امتیاز نهایی تأثیری نخواهد گذاشت.

معیار	مشخصه	مقدار کمی	توضیح
نیازهای امنیتی	کم (L)	۰/۵	از بین رفتن محرمانگی، جامعیت، در دسترس‌پذیری تأثیر محدودی روی سازمان و افرادی که با آن در ارتباط هستند (کارکنان، مشتریان) می‌گذارد.
	متوسط (M)	۱	از بین رفتن محرمانگی، جامعیت، در دسترس‌پذیری تأثیر سنگینی روی سازمان و افرادی که با آن در ارتباط هستند (کارکنان، مشتریان) می‌گذارد.
	زیاد (H)	۱/۵۱	از بین رفتن محرمانگی، جامعیت، در دسترس‌پذیری تأثیر فاجعه‌انگیزی روی سازمان و افرادی که با آن در ارتباط هستند (کارکنان، مشتریان) می‌گذارد.
	تعریف‌نشده (ND)	۱	با تخصیص این مقدار به معیار، این معیار روی امتیاز تأثیری نخواهد گذاشت.

٤-۲. جامعهٔ آماری و نمونهٔ آماری

جامعهٔ آماری مورد استفاده در این تحقیق را خبرگان، متخصصان و کارشناسان حوزهٔ امنیت اطلاعات و شبکه تشکیل می‌دهند. در این پژوهش از آنجا که به نظرات مجموعه‌ای از خبرگان برای ارزیابی شاخص‌های چارچوب پیشنهادی تحقیق نیاز بوده، از روش نمونه‌گیری قضاوتی (تخصصی) استفاده شده است. نمونه‌گیری قضاوتی مستلزم گزینش بخشی از جامعه است که اعضای آن بر پایهٔ داوری شخص پژوهنده مشخص می‌شود (دانایی‌فر و دیگران ۱۳۸۷). این روش در پی جمع‌آوری داده‌ها و دیدگاه‌های افرادی است که در ارتباط با موضوع مورد بررسی دارای آگاهی و تجربهٔ مؤثر می‌باشند. معیارهای نمونه‌گیری قضاوتی در این پژوهش عبارتند از: تجربهٔ کاری در حوزهٔ امنیت اطلاعات و شبکه، تدریس در مراکز علمی و دانشگاهی در زمینهٔ موضوع مورد نظر، ارائه تألیفات علمی (مقاله، پایان‌نامه، کتاب) در حوزهٔ مربوط. بر اساس روش نمونه‌گیری قضاوتی، ۷۵ نفر با مشخصات اشاره‌شده شناسایی گردیده و از طریق حضوری و پست الکترونیک تعداد ۷۵ نسخه پرسشنامه میان این افراد توزیع گردید که در نهایت تعداد ۴۰ پرسشنامه جمع‌آوری شده و در تحلیل‌ها مورد استفاده قرار گرفت (نرخ بازگشت پرسشنامه برابر ۵۳/۳ درصد).

٤-٣. روایی و پایایی

برای حصول اطمینان از روایی پرسشنامه، ویرایش اولیهٔ آن جهت اخذ نظر به پنج تن از استادان صاحب‌نظر در حوزهٔ فناوری و امنیت اطلاعات و شبکه ارسال و پس از اعمال اصلاحات لازم مورد استفاده قرار گرفت. به‌منظور تعیین پایایی پرسشنامه نیز روش آلفای کرونباخ به کار رفت. با استفاده از نرم‌افزار SPSS آلفای کرونباخ مجموعهٔ سؤال‌های 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 شاخص‌های انتخابی نیز به‌طور مجزا مقدار آلفای کرونباخ محاسبه گردید. در این مرحله نیز مقادیر به‌دست آمده بیشتر از حد قابل قبول ۰/۷ (Nunnally et al 1994) بود. مقادیر مربوط به هر یک از زیرمجموعه‌ها در جدول شماره ۸ نمایش داده شده است.

جدول ۸. چارچوب نظری تحقیق

	معیار	توضیحات
معیارهای پایه‌ای	بردار دسترسی	شناسایی چگونگی دستیابی و بعد فاصله حمله‌کننده برای دسترسی به شبکه
	پیچیدگی دسترسی	میزان مهارت و استعداد مورد نیاز برای بهره‌برداری از اطلاعات، محیط و سیستم‌های موجود در شبکه پس از به‌دست آوردن دسترسی
	تصدیق اصالت	تعداد دفعاتی که حمله‌کننده باید پیش از دسترسی به هدف و بهره‌برداری از آن تصدیق اصالت کند
	تصدیق فعالیت	تعداد و تنوع روش‌های قابل استفاده برای عدم انکار فعالیت‌های انجام‌شده در شبکه
	تأثیر بر محرمانگی	میزان اثر بهره‌بردای موفق از یک آسیب‌پذیری شبکه بر افشا و استفاده از اطلاعات محرمانه در محیط شبکه
	تأثیر بر امنیت ارتباطات	تعداد لایه‌های امنیتی که برای ایجاد امنیت ارتباطات به‌کار برده می‌شود
	تأثیر جامعیت	میزان تغییری که حمله‌کننده می‌تواند در اطلاعات، محیط و سیستم‌های موجود در شبکه پس از به‌دست آوردن دسترسی اعمال نماید
	در دسترس‌پذیری	میزان تغییری که حمله‌کننده می‌تواند در دسترسی کاربران به شبکه پس از نفوذ به شبکه اعمال نماید

	معیار	توضیحات
معیارهای موقتی	قابلیت	میزان دسترسی عمومی به نرم‌افزارها، کدها و تکنیک‌هایی که برای نفوذ و آسیب‌رسانی به شبکه‌ها قابل استفاده است
	بهره‌برداری	
	سطح ترمیم	راهکارهای سازمانی در جهت مدیریت و مواجهه با آسیب‌های ایجادشده
	اطمینان از گزارش	میزان اطمینان از وجود آسیب‌پذیری و اعتبار جزئیات فنی آن
معیارهای محیطی	میزان خسارت بالقوه	میزان خسارت ناشی از حمله و یا دسترسی غیرمجاز به شبکه (شامل انواع خسارت اقتصادی، کارآیی، بازده و ...)
	توزیع هدف	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)

٤-٤. تحلیل داده‌ها

بررسی متغیرهای جمعیت‌شناختی پاسخ‌دهندگان به سؤالات پرسشنامه نشان می‌دهد که ۲۸/۴ درصد از پاسخ‌دهندگان زن و۷۱/۶ 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=۰/۶۵۳) که بزرگتر از مقدار قابل قبول ۰/۶ (Hair 1998) بوده و عدد معناداری آزمون بارتلت (sig =۰/۰۰) که کمتر از ۰/۰۵ است، می‌توان تناسب داده‌ها برای اجرای تحلیل عاملی و کافی‌بودن اندازهٔ نمونهٔ 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 نشان‌دهندهٔ 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 به‌خود اختصاص داده و معیارهای موقتی و معیارهای محیطی به‌ترتیب در اولویت‌های بعدی قرار می‌گیرند. از آنجا که بارهای عاملی سؤالات با عامل مربوط به‌خود بالای ۰/۵۰ و با عامل‌های دیگر کمتر از ۰/۵۰ می‌باشد، روایی واگرا 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 تبیین‌شده = ۳۰/۱۴۳) و معیارهای موقتی (واریانس تبیین‌شده= ۱۶/۰۲۸) و معیارهای محیطی (واریانس تبیین‌شده= ۱۵/۸۱۱) دارای اولویت‌های بعدی هستند.

جدول ۹. نتایج تحلیل داده‌ها

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

بر اساس موارد مندرج در جدول شماره ۹ مشاهده می‌گردد که میانگین تمامی ابعاد بیشتر از عدد ۳ می‌باشد و این مقدار نشان دهندهٔ پاسخ مثبت به ابعاد است. بر اساس نتایج

حاصل از تحلیل عاملی درج‌شده در جدول شماره ۹ مشخص می‌گردد که بار عاملی تمامی معیارهای مورد آزمون بیشتر از ۰/۵ می‌باشد و تمامی معیارهای انتخابی در تبیین آسیب‌پذیری‌های شبکه نقش دارند. واریانس کل تبیین‌شده توسط ابعاد مدل برابر با ۶۱/۹۸ درصد بوده که نشانگر مطلوبیت چارچوب پیشنهادی در تبیین آسیب‌پذیری‌های شبکه می‌باشد. بر اساس موارد مندرج در همین جدول، معیارهای پایه‌ای با بار عاملی ۳۰/۱۴۳ بیشترین نقش را در تبیین آسیب‌پذیری‌های شبکه دارا بوده و پس از آن بُعد محیطی با بار عاملی ۱۶/۰۲۸، و بُعد موقتی با بار عاملی ۱۵/۸۱۱ نقش‌های بعدی در تبیین آسیب‌پذیری‌های شبکه را به‌خود اختصاص داده‌اند. این مقادیر نشانگر میزان اهمیت هر یک از این ابعاد در شناسایی آسیب‌پذیری‌های شبکه می‌باشد. 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 آسیب‌پذیری شبکه را دارا می‌باشند.

٤-٥. بررسی یک نمونهٔ عملی

در این بخش به‌منظور تعیین نحوهٔ محاسبات کمی در خصوص میزان آسیب‌پذیری شبکه در راهکار پیشنهادی، به بررسی یک نمونهٔ عملی پرداخته شده است. نمونهٔ عملی مورد نظر دارای فعالیت تولیدی در عرصهٔ صنعت کاشی و سرامیک بوده و دارای یک محیط تولیدی و دو دفتر منطقه‌ای می‌باشد. تعداد کاربران فعال که از شبکهٔ این مجموعه استفاده می‌نمایند، ۱۵۳ نفر در محیط تولیدی، ۲۷ نفر در دفتر متطقه‌ای الف و ۵۴ نفر در دفتر منطقه‌ای ب می‌باشد. ارتباط میان این سه موقعیت جغرافیایی از طریق شبکه MPLS و ارتباطات بی‌سیم تأمین می‌گردد. این مجموعه اخیراً اقدام به تأمین سیستم‌های ERP تحت وب نموده که ۷۰ درصد از ماژول‌های سیستم خریداری‌شده پیاده‌سازی و عملیاتی شده است. این مجموعه به‌منظور افزایش ضریب امنیت اطلاعات سازمانی خود در نظر دارد طرحی به‌نام طرح جامع افزایش ضریب امنیت اطلاعات و شبکه را در سازمان خود اجرا نماید. با توجه به هماهنگی صورت‌پذیرفته با این مجموعه و معرفی روش پیشنهادی در این مقاله مقرر گردید در راستای اولویت‌بندی اجرای طرح افزایش ضریب امنیت اطلاعات سازمانی نسبت به محاسبهٔ میزان آسیب‌پذیری شبکهٔ این مجموعه برای موقعیت تولیدی و

دفاتر منطقه‌ای اقدام گردد. بدین‌منظور یک جلسهٔ هم‌اندیشی برای معرفی روش پیشنهادی با حضور متخصصان واحد فناوری اطلاعات برگزار گردید. پس از این جلسهٔ و تشریح روش، اطلاعات لازم با همکاری کارشناسان واحد فناوری اطلاعات جمع‌آوری شد. خلاصهٔ نتایج به‌دست آمده در جدول شماره ۱۰ درج گردیده است.

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

معیار		محیط تولیدی		دفتر منطقه‌ای الف		دفتر منطقه‌ای ب	
		وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی
معیارهای پایه	بردار دسترسی	شبکه LAN داخلی	۱	شبکه LAN داخلی	۰,۶۴۶	شبکه LAN داخلی	۱
		بی‌سیم W-LAN				بی‌سیم W-LAN	
		شبکه اینترنت		شبکه اینترنت		شبکه اینترنت	
	پیچیدگی دسترسی	زیاد (H)	۰,۳۵	متوسط (M)	۰,۶۱	متوسط (M)	۰,۶۱
	تصدیق اصالت	واحد (S)	۰,۵۶	واحد (S)	۰,۵۶	واحد (S)	۰,۵۶
	تصدیق فعالیت	واحد (S)	۰,۵۶	واحد (S)	۰,۵۶	واحد (S)	۰,۵۶
	تأثیر بر محرمانگی	ناقص (P)	۰,۲۷۵	ناقص (P)	۰,۲۷۵	ناقص (P)	۰,۲۷۵
	تأثیر بر امنیت ارتباطات	واحد (S)	۰,۵۶	واحد (S)	۰,۵۶	واحد (S)	۰,۵۶
	تأثیر جامعیت	ناقص(P)	۰,۲۷۵	هیچ (N)	۰	هیچ (N)	۰
	در دسترس‌پذیری	ناقص (P)	۰,۲۷۵	کامل (C)	۰,۶۶	کامل (C)	۰,۶۶

معیار		محیط تولیدی		دفتر منطقه‌ای الف		دفتر منطقه‌ای ب	
		وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی	وضعیت نمونه در مشخصه	مقدار کمی
معیارهای موقتی	قابلیت بهره‌برداری	در حال کار (F)	۰,۹۵	در حال کار (F)	۰,۹۵	در حال کار (F)	۰,۹۵
	سطح ترمیم	دور زدن آسیب‌پذیری (W)	۰,۹۵	ترمیم آسیب‌پذیری رسمی (OF)	۰,۸۷	ترمیم آسیب‌پذیری موقتی (TF)	۰,۸۷
	اطمینان از گزارش	تعریف‌نشده (ND)	۱	تعریف‌نشده (ND)	۱	تعریف‌نشده (ND)	۱
معیارهای محیطی	میزان خسارت بالقوه	متوسط ـ زیاد (MH)	۰,۴	کم (L)	۰,۱	متوسط ـ زیاد (MH)	۱
	توزیع هدف	کم (L)	۰,۲۵	هیچ (N)	۰	هیچ (N)	۰
	نیازهای امنیتی	متوسط (M)	۱	کم (L)	۰,۵	کم (L)	۰,۵

با وارد نمودن مقادیر مندرج در جدول شماره ۱۰ در فرمول‌های محاسباتی ارائه‌شده در روش پیشنهادی (بر اساس نحوهٔ محاسبهٔ ارائه‌شده در شکل شماره ۲) مقادیر معیارهای پایه، موقتی و محیطی برای شبکهٔ این مجموعه در سه موقعیت تولیدی، دفتر منطقه‌ای الف و دفتر منطقه‌ای ب محاسبه و مقادیر و محاسبات آن در شکل شماره ۳ درج گردید.

مقادیر معیارهای پایه، موقتی و محیطی در محیط تولیدی
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 **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
مقادیر معیارهای پایه، موقتی و محیطی در دفتر منطقه‌ای الف
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 **TemporalScore = round_to_1_decimal (4.4*0.95*0.87*1) = 3.6** *با توجه به اینکه میزان توزیع هدف برابر هیچ (N) می‌باشد، محاسبه معیار محیطی لازم نمی‌باشد.
مقادیر معیارهای پایه، موقتی و محیطی در دفتر منطقه‌ای ب
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 **TemporalScore = round_to_1_decimal (4.8*0.95*0.87*1) = 4.0** * با توجه به اینکه میزان توزیع هدف برابر هیچ (N) می‌باشد، محاسبه معیار محیطی لازم نمی‌باشد.

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

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

در بخش معیار پایه، دلیل اصلی بالابودن درجهٔ آسیب‌پذیری شبکهٔ دفتر منطقه‌ای ب نسبت به محیط تولیدی را می‌توان در مقادیر معیارهای پیچیدگی دسترسی و در دسترس‌پذیری دانست. در همین حال، دفتر منطقه‌ای الف به‌دلیل 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 بالابودن درجهٔ آسیب‌پذیری شبکهٔ دفتر منطقه‌ای الف و ب نسبت به محیط تولیدی را می‌توان در وضعیت معیار سطح ترمیم جستجو نمود. در همین حال، و با توجه به تأثیر معیار پایه در معیار موقتی، به‌دلیل بالاتربودن مقدار معیار پایه در دفتر منطقه‌ای ب نسبت به دفتر منطقه‌ای الف، مقدار معیار موقتی آن نسبت به دفتر منطقه‌ای الف بالاتر خواهد بود. با توجه به محاسبات انجام‌شده می‌توان نتیجه گرفت که مجموعهٔ مذکور می‌بایست اولویت طرح افزایش ضریب امنیت اطلاعات را برای دفاتر منطقه‌ای ب، الف و سپس محیط تولیدی خود اجرا نماید.

۵. نتیجه‌گیری

این مقاله تلاش نمود بر پایهٔ معماری امنیت ITU-TX-805 روشی به‌منظور محاسبهٔ کمی آسیب‌پذیری‌های شبکه تحت عنوان NCVSS ارائه نماید. برای دستیابی به هدف موضوع مقاله ضمن بررسی گستردهٔ ادبیات مربوط به آسیب‌پذیری شبکه و مدل‌های مطرح برای کمی‌سازی مقادیر آسیب‌پذیری‌ها، پرسشنامه‌ای تدوین و برای ارزیابی اعتبار شاخص‌های استخراج‌شده در اختیار کارشناسان و خبرگان در حوزهٔ امنیت قرار گرفت. نتایج اجرای تحلیل عاملی بر روی داده‌های به‌دست آمده، نشان‌دهندهٔ تأثیر مؤلفه‌های آسیب‌پذیری بر روی میزان آسیب‌پذیری شبکه‌های رایانه‌ای است. بر اساس نتایج این تحقیق معیارهای پایه‌ای (شامل بردار دسترسی، پیچیدگی دسترسی، تصدیق اصالت، تصدیق فعالیت، تأثیر بر محرمانگی، تأثیر بر امنیت ارتباطات، تأثیر جامعیت، و در دسترس‌پذیری) بیشترین نقش را در تبیین واریانس آسیب‌پذیری‌های شبکه دارا می‌باشند (واریانس تبیین‌شده= ۳۰/۱۴۳). از سوی دیگر، معیارهای موقتی (شامل قابلیت بهره‌برداری، سطح ترمیم، اطمینان از گزارش) با واریانس تبیین‌شده= ۱۶/۰۲۸ و معیارهای موقتی (شامل میزان خسارت بالقوه، توزیع هدف، نیازهای امنیتی) با واریانس تبیین‌شده= ۱۵/۸۱۱ در اولویت‌های بعدی قرار دارند.

بر اساس روش پیشنهادی در این تحقیق امکان مدیریت مؤثر آسیب‌پذیری‌ها از طریق کمی‌سازی مقادیر آسیب‌پذیری‌ها فراهم گردیده است. با توجه به نبودِ روش‌های محاسبهٔ کمی آسیب‌پذیری‌ها در حوزه شبکه‌های رایانه‌ای و نیاز عملیاتی متخصصان این حوزه، روش پیشنهادی در این تحقیق می‌تواند در عین سادگی و سهولت استفاده به‌عنوان یک

روش ابتکاری کارآمد و مؤثر در محاسبهٔ میزان آسیب‌پذیری‌های شبکهٔ رایانه‌ای مورد استفاده قرار گیرد.

تشکر و قدردانی

پژوهشگران بر خود لازم می‌دانند از همکاری و مساعدت سرکار خانم مهندس فاطمه آل‌آقا که در انجام این تحقیق همکاری داشته‌اند، مراتب سپاس خود را اعلام نمایند.

٦. فهرست منابع

امامی، ساره‌سادات و جعفرهادی جعفریان. ۱۳۸۸. *محاسبهٔ درجهٔ آسیب‌پذیری سیستم‌ها*. اولین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات، تهران.

امیدیان، علیرضا، علی نورالهی راوری و رسول جلیلی. ۱۳۸۸. *دسته‌بندی آسیب‌پذیری‌های شناخته‌شده در سیستم‌های مدیریت پایگاه داده‌ها*. اولین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات، تهران.

حاجیان، سارا، فرامرز هندسی، مهدی برنجکوب، سیدهادی هاشمی و پیمان گلشنی. ۱۳۸۸. *ارائه یک رده‌بندی جدید برای آسیب‌پذیری‌های شبکه*. اولین کنفرانس حوادث و آسیب‌پذیری‌های امنیت فضای تبادل اطلاعات، تهران.

دانایی‌فر، حسن، سیدمهدی الوانی و عادل آذر. ۱۳۸۷. *روش‌شناسی کمی در مدیریت: رویکردی جامع، اول*. تهران: صفار.

صدقی، عباس، سیدرضا سیدجوادین، داود مطلبی، سیدجابر حسینی و حمیدرضا یزدانی. ۱۳۸۸. بررسی مقایسه‌ای مدل‌های 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.

Corcalciuc, 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.

Fruhwirth, 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 Confernece 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. Chandrashekhar 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. Hanyurwinfura. 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. Barekatain. 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.

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

Mohammad Hossein Sherkat[1] | **Shahriyar Mohammadi**[2] | **Mona JamiPour**[3]

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

Iranian Research Institute for Science and Technology
ISSN 2251-8223
eISSN 2251-8231
Indexed in SCOPUS, ISC & LISA
Vol.29 | No.4 | pp: 1107-1145
Summer 2014

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