INSO-ISO-IEC
15408-1
1st. Edition
Identical with
ISO/IEC15408-1, 2009
2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ایران ایزو آی ای سی
۱۵۴۰۸-۱
چاپ اول
۱۳۹۱

فن‌آوری اطلاعات- فنون امنیتی- معیارهای ارزیابی امنیت فناوری اطلاعات- قسمت ۱- معرفی و مدل عمومی

Information technology-Security techniques - Evaluation criteria for IT security- Part 1: Introduction and general model

ICS:35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (واسنجی) وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2 - International Electrotechnical Commission
3- International Organization of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فن‌آوری اطلاعات- فنون امنیتی- معیارهای ارزیابی امنیت فناوری اطلاعات-قسمت ۱-معرفی و مدل »

رئیس:	**سمت و/ یا نمایندگی**
سپیده صفایی (کارشناس کامپیوتر)	کارشناس نرم‌افزار شرکت داده‌کاوان امن‌پرداز
دبیر:	
علیرضا منافی (کارشناس ارشد رایانه)	مدیر عامل شرکت امن‌افزار گستر شریف
اعضاء: (اسامی به ترتیب حروف الفبا)	
اخوان نیاکی، سید انوشیروان (کارشناس ارشد مدیریت IT)	مشاور مدیر عامل و مدیر مرکز مدیریت دانش و داده کاوی شرکت ایزایران
علی محمد ملایری، عصمت (کارشناس ارشد نرم‌افزار)	مدرس دانشگاه آزاد ملایر
مروجی، سجاد (کارشناس ارشد رایانه)	مدرس دانشگاه
سید علیرضا مهدوی (کارشناس ارشد مدیریت IT)	مشاور شرکت داده‌پردازان آبشار
ولی،ناصر (کارشناس ارشد نرم‌افزار)	کارشناس IT کمیته امداد امام خمینی

فهرست مندرجات

پیش گفتار

استاندارد« فناوری اطلاعات- فنون امنیتی- معیارهای ارزیابی امنیت فناوری اطلاعات قسمت۱- معرفی و مدل عمومی» نخستین بار در سال ۱۳۸۷ تدوین شد. این استاندارد بر اساس پیشنهادهای رسیده و بررسی توسط موسسه استاندارد و تحقیقات صنعتی ایران و تایید کمیسیون‌های مربوط برای اولین بار مورد تجدید نظر قرار گرفت و در دویست و شصت و نهمین اجلاس کمیته ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۹۱/۱۲/۱۲ تصویب شد. اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ ، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائهٔ شود، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت . بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی استفاده کرد.

این استاندارد جایگزین استاندارد ملی ایران شماره ISIRI-ISO/IEC 15408-1سال ۱۳۸۷ است.

منبع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC15408-1, 2009 Information technology — Security techniques — Evaluation criteria for IT security part 1 – Introduction and general model

مقدمه

این استاندارد ملی یکی از مجموعه استانداردهای ملی ایران به شماره ISIRI-ISO/IEC 15408 است. این استاندارد ملی با توجه به نتایج ارزیابی امنیتی مجوز مقایسه را می‌دهد. به این منظور مجموعه‌ای از نیازمندی‌ها

را برای توابع امنیتی محصولات و سامانه‌های فن‌آوری اطلاعات (IT) [1] آماده کرده و استفاده از آنها را با توجه به ارزیابی امنیتی تضمین می‌کند. این محصولات ممکن است در سخت افزار، میان افزار و یا نرم افزار اجرا شوند.
فرایند ارزیابی، سطح محرمانگی توابع امنیتی محصولات و سامانه‌ها و اندازه‌های تضمینی جهت به‌کارگیری این نیازمندی‌ها را مشخص می‌کند. نتایج ارزیابی می‌تواند به مشتریان کمک می‌کند که تعیین کنند آیا محصول IT نیازهای امنیتی آنها را برآورده می‌کند.
این استاندارد ملی می‌تواند به عنوان راهنما در جهت توسعه، ارزیابی یا تهیه محصولات IT که نیازمند توابع امنیتی هستند، استفاده شود.
این استاندارد ملی به صورت حساب شده‌ای انعطاف پذیر است، گستره‌ای از روش‌های ارزیابی را برای به‌کارگیری در گستره‌ای از ویژگی‌های امنیتی از طیف وسیعی از محصولات فناوری اطلاعات قادر می‌سازد. بنابراین به کاربران این استاندارد ملی هشدار داده شده است که این انعطاف پذیری سوء استفاده نیست. به عنوان مثال، استفاده از این استاندارد ملی در رابطه با روش‌های ارزیابی نامناسب، خواص امنیتی بی ربط یا نامناسب محصولات IT، ممکن است منجر به نتایج ارزیابی بی معنی شود.
در نتیجه، این واقعیت که یک محصول فناوری اطلاعات مورد ارزیابی قرار گرفته شده است تنها در چهارچوب کاری ویژگی‌های امنیتی که ارزیابی شده است و روش‌های ارزیابی که مورد استفاده قرار گرفته معنا دارد. مقامات ارزیابی توصیه به دقت در بررسی محصولات، ویژگیها و روشها برای تصمیم گیری در این مورد که ارزیابی نتایج معنی دار را فراهم می‌کند، یا خیر شده اند .علاوه بر این، خریداران محصولات ارزیابی شده توصیه به در نظر گرفتن این زمینه به تعیین اینکه آیا این محصول مورد بررسی مفید و کاربردی برای موقعیت خاص و نیازهای آنها هست یا خیر.
این استاندارد ملی به عنوان مرجعی در جهت حفاظت در مقابل افشا، اصلاح و نابودسازی غیر مجاز، استفاده می‌شود. مقوله حفاظت مرتبط با ضعف‌های امنیتی به طور عمده در سه حوزه محرمانگی، صحت، و دسترس‌پذیری شناخته شده است. این استاندارد ملی در این سه حوزه نیز کاربرد دارد. SO / IEC 15408 در رابطه با خطرات ناشی از فعالیت‌های انسانی (کدهای مخرب و یا چیزهای دیگر) و خطرات ناشی از فعالیت‌های غیر انسانی نیز کاربرد دارد.جدای از امنیت فناوری اطلاعات، این استاندارد ملی ممکن است در زمینه‌های دیگری از فناوری اطلاعات نیز کاربرد داشته باشد اما هیچ ادعایی در رابطه با کاربرد در این زمینه‌ها نمی‌کند.
مباحث خاص به دلیل در برداشتن تکنیک‌های تخصصی یا به دلیل اینکه تا حدودی برای امنیت فناوری اطلاعات به عنوان موضوعاتی جانبی مطرح می‌شوند، به عنوان حوزه این استاندارد ملی مد نظر قرار می‌گیرند.
این استاندارد ملی برای موارد زیر کاربرد دارد:
الف- این استاندارد ملی در برگیرنده معیار ارزیابی امنیت وابسته به اقدامات امنیتی اجرایی نمی‌باشد، این اقدامات همچنین به طور مستقیم به اقدامات امنیتی فناوری اطلاعات مربوط نمی‌شوند.اگر چه، اینگونه تشخیص داده شده است که امنیت قابل توجه را اغلب می توان از طریق اقدامات اجرایی مانند کنترل‌های سازمانی، پرسنلی، فیزیکی و رویه‌ای ایجاد نمود.

1 -Information Technology

ب- ارزیابی جنبه‌های فیزیکی فنی امنیت فناوری اطلاعات مانند کنترل صدور جریان الکترومغناطیسی به طـور خاص تحت پوشش قرار نمی‌گیرد، این در حالی است که بسیاری از مفاهیم مورد نظر، برای این سطح، قابل اجرا خواهند بود.

پ- این استاندارد ملی به روش ارزیابی که تحت آن ضوابط باید به کار رود اشاره نمی‌کند. این روش در ISO/IEC 18045آورده شده است.

ت- این استاندارد ملی به چارچوب اداری و قانونی که تحت آن معیارها ممکن است توسط مقامات ارزیابی اعمال شود اشاره نمی‌کند.با این حال، انتظار می‌رود که این استاندارد ملی در زمینه چنین چارچوبی به منظور ارزیابی مورد استفاده قرار خواهد گرفت.

ث- رویه‌های به کارگیری نتایج ارزیابی در تعیین اعتبار خارج از حوزه این استاندارد ملی می باشد. تعیین اعتبار ، فرآیندی اجرایی بوده که مجوز عملکرد محصول فناوری اطلاعات در محیطی کاملا عملیاتی ارائه می شود. ارزیابی بر روی قسمت‌های امنیتی فناوری اطلاعات محصول (یا مجموعه وابسته به آن) برای تمام محیط عملیاتی که دربرگیرنده تمام قسمت‌های غیر از فن‌آوری اطلاعات می‌باشد، اعطا شده است. نتایج فرآیند ارزیابی در نهایت، ورودی ارزشمندی برای فرآیند تعیین اعتبار می باشد. اگرچه، از آنجایی که سایر فنون، جهت ارزیابی ویژگی‌های امنیتی سامانه یا محصول و ارتباط آنها با قسمت‌های امنیتی فناوری اطلاعات، مناسب‌تر می‌باشند، اعتبارنامه‌ها باید تمهیدات جداگانه‌ای را برای این جوانب ایجاد کنند.

ج- موضوع معیار برای ارزیابی کیفیت‌های ذاتی الگوریتم‌های رمز نگاری شده در این استاندارد ملی تحت پوشش قرار نمی گیرد. ارزیابی مستقلی از ویژگی‌های ریاضی رمزنگاری مورد نیاز می‌باشد. طرح کلی ارزیابی که این استاندارد ملی تحت آن انجام می‌شود باید تمهیداتی را برای چنین ارزیابی‌هایی در نظر بگیرد.

مجموعه اصطلاحات ISO، مانند «can»، «informative»، «may»، «normative»، «shall» و «should» از سند که در راهنمای ISO/IEC قسمت ۲ آورده شده است استفاده کرده است. توجه دارید که «should» هنگامی که در این استاندارد استفاده میشود یک معنای قابل کاربرد اضافه نیز دارد.نکته زیر را ببینید.تعریف زیر برای استفاده «should» در ISO/IEC 15408 آورده شده است.

Should

در متن اصلی، «should» نشان‌دهنده این امر است که « در میان چندین احتمال، یکی به عنوان احتمال مناسب، بدون اشاره نمودن یا مستثنی نمودن سایر موارد، پیشنهاد می‌شود یا اینکه راه کار خاصی ترجیح داده می‌شود. اما لزوما استفاده از آن، مورد نیاز نمی‌باشد. » (دستورالعمل‌های ISO/IEC، قسمت دوم)

یادآوری- این استاندارد ملی تفسیر می‌کند «لزوما لازم نیست» به این معنی که انتخاب از احتمال دیگر نیاز به توجیه این دارد که چرا گزینه ارجح انتخاب نشد.

فناوری اطلاعات- فنون امنیت- معیار ارزیابی امنیت فناوری اطلاعات-قسمت۱- معرفي و مدل عمومي

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد تعیین مفاهیم کلی و اصول امنیت ارزیابی فناوری اطلاعات می‌باشد و مدل ارزیابی ارائه شده توسط قسمت‌های مختلف استاندارد ملی را مشخص می‌کند که در تمامیت خود به معنای استفاده به عنوان پایه ای برای ارزیابی ویژگی‌های امنیتی محصولات فناوری اطلاعات می‌باشد.

این استاندارد ملی یک نمای کلی از تمام قسمت‌های این استاندارد ملی را فراهم می‌کند. این استاندارد ملی قسمت‌های مختلف از استاندارد را شرح می‌دهد. اصطلاحات و کوته‌نوشت‌هایی که در تمام قسمت‌های این استاندارد ملی مورد استفاده قرار می‌گیرد را تعریف می‌کند، مفهوم اصلی یک هدف امنیتی (TOE) را ایجاد می‌کند ، زمینه ارزیابی و توصیف مخاطبانی که در آن ارزیابی معیار مورد خطاب قرار گرفته اند را شرح می‌دهد .مقدمه ای بر مفاهیم پایه امنیت لازم برای ارزیابی محصولات فناوری اطلاعات نیز داده شده است.

این استاندارد ملی عملیات مختلف عناصرعملیاتی و تضمین که در ISO / IEC 15408-2 و ISO / IEC 15408-3 آورده شده است را تعریف می‌کند که ممکن است از طریق استفاده از عملیات مجاز طراحی شده باشند.

مفاهیم کلیدی از رخ‌نمون محافظتی (PP[1])، بسته‌های نیازمندی‌های امنیت و موضوع انطباق مشخص شده و پیامدهای ناشی از ارزیابی و نتایج ارزیابی شرح داده شده است. این قسمت از ISO / IEC 15408 به رهنمودهایی برای تعیین اهداف امنیتی (ST) میپردازد و شرحی از ساختار اجزای سازنده در سراسر مدل را فراهم می‌کند .اطلاعات عمومی در مورد روش ارزیابی در ISO / IEC 18045 داده می‌شود و هدف از طرح ارزیابی ارائه شده است.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود. در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ و انتشار به آنها ارجاع داده شده است، همواره آخرین تجدید نظر و اصلاحیه‌های بعدی آنها مورد نظر است.

استفاده از مرجع زیر برای این استاندارد الزامی است:

2-1 ISO/IEC 15408-2, Information technology - Security techniques - Evaluation criteria for IT security - Part 2:Security functional components[2]

2-2 ISO/IEC 15408-3, Information technology - Security techniques - Evaluation criteria for IT security - Part 3:Security assurance components [3]

2-3ISO/IEC 18045, Information technology - Security techniques - Methodology for IT security evaluation

---

1 - Protection Profile

۲ - برای استاندارد بین‌المللی ۲-۱۵۴۰۸ سال ۲۰۰۵ استاندارد بین‌المللی به شماره ۲-۱۵۴۰۸ نشر شده است .

۳ - برای استاندارد بین‌المللی ۳-۱۵۴۰۸ سال ۲۰۰۸ استاندارد بین‌المللی به شماره ۳-۱۵۴۰۸ نشر شده است

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

یادآوری- تنها روش خاصی را که در این استاندارد ملی مورد استفاده قرار گرفته است را شامل می‌شود. برخی از ترکیب‌های اصطلاحات مشترک به کار رفته در این استاندارد ملی ، با وجود اینکه چندان ارزشی در این بند ندارند، جهت واضح نمودن متن، توضیح آنها در جایی که مورد استفاده قرار می‌گیرند، داده می‌شود.

۳-۱ اصطلاحات و تعاریف مشترک در ISO/IEC 15408

۳-۱-۱

عملیات نامطلوب

عملیات انجام شده توسط یک عامل تهدید بر روی یک دارایی .

۳-۱ -۲

دارایی‌ها[1]

اطلاعات یا منابعی که از طریق اقدامات متقابل هدف ارزیابی (TOE) پشتیبانی می‌شوند.

۳-۱ -۳

واگذاری[2]

ویژگی پارامتری شناخته شده در یک مؤلفه(از این استاندارد ملی) می‌باشد.

۳-۱ -۴

ضمانت

زمینه ای برای اعتماد به این که TOE منطبق با SFR باشد.

۳-۱ -۵

عامل بالقوه حمله[3]

عامل بالقوه مشخص شده برای موفقیت در یک حمله باید بر طبق تخصص حمله کننده، منابع و انگیزه مطرح شده آغاز شود.

۳-۱ -۶

افزایش

اضافه شدن یک یا چند نیازمندی به یک بسته را می‌گویند.

۳-۱ -۷

داده تائید

اطلاعات به کارگرفته شده جهت تغییر هویت مطالبه شده از کاربر می‌باشد.

---

1 - Assets

2- Assignment

3 -Attack potential

۳-۱-۸

کاربر مجاز[1]

کاربری که بر طبق SFRS باید عملیاتی را انجام دهد.

۳-۱-۹

گروه

دسته‌ای از خانواده‌ی این استاندارد ملی که هدف مشترکی را دارند.

۳-۱-۱۰

منسجم

صورت منطقی منظم و معنای قابل تشخیص داشتن.

یادآوری- برای مستندسازی، این آدرس، متن واقعی و ساختار سند، به لحاظ اینکه آیا توسط مخاطبان هدف خود قابل فهم است یا خیر؟

۳-۱-۱۱

کامل

دارایی‌های که در آن تمام قسمت‌های لازم از هستار ارائه شده است.

۳- ۱-۱۲

مؤلفه

کوچکترین مجموعه ی قابل انتخاب از عناصر که ممکن است بر اساس الزامات باشد.

۳-۱-۱۳

بسته تضمین ترکیبی

بسته تضمین متشکل از الزامات برگرفته از ISO / IEC 15408-3 (عمدتا از طبقه ACO)، یک نقطه دوباره تعریف شده مقیاس تضمین ترکیب در این استاندارد ملی را نمایش میدهد.

۳-۱-۱۴

تایید

اظهار کردن این موضوع که بعضی چیزها به جزییات با یک تصمیم گیری مستقل از کفایت مرور شده‌اند.

یادآوری- سطح دقت مورد نیاز بستگی به ماهیت موضوع دارد.این واژه تنها برای عملیات ارزیاب به کار می‌رود.

1 -Authorised user

۳-۱-۱۵

اتصال

ویژگی هدف ارزیابی (TOE) که امکان تعامل با هستارهای فناوری اطلاعات که برای هدف ارزیابی به عنوان عاملی خارجی محسوب می‌شوند را فراهم می‌کنند. این امر شامل تبادل داده‌ها از طریق سیم یا بدون سیم در هر فاصله‌ای در هر محیط یا پیکربندی می‌باشد.

۳-۱-۱۶

نامتناقض

ارتباط بین دو یا بیشتر هستارهایی که هیچ تناقضات آشکار میان این هستارها وجود ندارد

۳-۱-۱۷

شمارنده ،فعل

ملاقات یک حمله جای یکه تاثیر یک تهدید ویژه، سبک شده اما لزوما ریشه کن نشده است.

۳-۱-۱۸

مطابقت قابل اثبات

رابطه بین یک ST و PP به طوری که ST یک راه حل برای حل مشکلات امنیتی کلی در PP فراهم کند.

۳-۱-۱۹

نشان دادن

ارائه یک نتیجه به دست آمده توسط یک تجزیه و تحلیل دقیق است که کمتر از یک«اثبات» است.

۳-۱-۲۰

وابستگی

ارتباط بین مولفه‌ها به طوری که اگر یک نیازمندی بر اساس مولفه‌های وابسته در PP، ST یا بسته است، یک نیازمندی بر اساس مولفه‌ای که وابسته است باید به طور طبیعی در ST،PP یا بسته باشد.

۳-۱-۲۱

شرح دادن

تامین جزییات خاص هر هستار

۳-۱-۲۲

تصدیق یک نتیجه خاص بر اساس تجزیه و تحلیل مستقل با هدف رسیدن به یک نتیجه گیری خاص.

یادآوری- استفاده از این واژه به معنی تجزیه و تحلیل واقعا مستقل است، معمولا در شرایطی که از هر گونه تجزیه و تحلیل قبلی انجام نشده باشد. در مقایسه با شرایط "تایید" یا "صحت" که این مفهوم را میرسانند که تجزیه و تحلیلی که در حال حاضر انجام شدن است نیازمند بازبینی است.

۳-۱-۲۳

محیط توسعه

محیطی که TOE در آن توسعه یافته است.

۲۴-۱-۳

مؤلفه

بیانیه غیر قابل تقسیم از یک نیاز امنیتی می‌باشد

۲۵-۱-۳

حصول اطمینان

تضمین یک رابطه عللی قوی بین عمل و عواقب آن.

یادآوری- هنگامی که این اصطلاح با استفاده از کلمه «راهنما» قبل از آن می‌آید نشان می‌دهد که ، بر اساس آن اقدام به تنهایی

نتیجه به طور کامل حتمی نیست.

۲۶-۱-۳

ارزیابی

ارزش‌یابی PP، ST یا TOE در مقابل معیاری تعیین شده است.

۲۷-۱-۳

سطح تضمین ارزیابی[1]

بسته‌ای که شامل مؤلفه‌های ضمانت از این استاندارد ملی - قسمت ۳ بوده و نشان دهنده یک حد معین بر روی این استاندارد ملی که یک بسته تضمین را تشکیل می‌دهد، معیار تضمین از پیش تعیین شده می‌باشد.

۲۸-۱-۳

ارزیابی قدرت

قسمت اصلی که استانداردها را تعیین می‌کند و نظارت بر کیفیت ارزیابی‌های انجام شده که توسط قسمت اصلی در یک اجتماع خاص جریان داشته است و این استاندارد ملی را برای آن جامعه با استفاده از طرح ارزیابی پیاده سازی می‌کند، نظارت می‌کند.

۲۹-۱-۳

طرح ارزیابی

چارچوب کاری اداری و مقرراتی که تحت آن، این استاندارد ملی با استفاده از قدرت ارزیابی در یک اجتماع خاص به کار گرفته میشود.

۳۰-۱-۳

جامع

خصوصیات رویکرد روشمندی که اتخاذ شده است که تجزیه و تحلیل و یا فعالیت با توجه به طرح ابهام را انجام دهد.

یادآوری- این اصطلاح در این استاندارد ملی با توجه به انجام تجزیه و تحلیل و یا فعالیت‌های دیگر استفاده می‌شود. این مربوط به «سیستماتیک» است، اما به طور قابل ملاحظه ای قوی تر، که در آن نشان می‌دهد که نه تنها یک رویکرد

1 -Evaluation assurance level

روشمند، به منظور انجام تجزیه و تحلیل و یا فعالیت با توجه به طرح ابهام اتخاذ شده است، بلکه این طرح بود که از آن پیروی شد، کافی است تا اطمینان حاصل شود که تمام راه‌های ممکن اعمال شده است.

۳-۱-۳۱

توضیح دادن

ارائه حسابداری استدلال که بر اساس آن یک دوره آموزشی از اقدامات در نظر گرفته میشود.

یادآوری -این اصطلاح متفاوت از هردو اصطلاح «توصیف» و «نشان دادن» است. این اصطلاح، برای پاسخ به سوال « چرا؟»در واقع بدون تلاش برای بحث در مورد این که این دوره آموزشی گزرانده شده لزوما مطلوب است، در نظر گرفته شده است.

۳-۱-۳۲

گسترش

اضافه نمودن الزامات عملیاتی ST یا پروفایل محافظتی(pp) که در قسمت ۲ از این استاندارد ملی و یا الزامات تضمین که در این استاندارد ملی-قسمت ۳ وجود ندارد.

۳-۱-۳۳

هستار خارجی[1]

هستار انسانی یا فناوری اطلاعات که احتمالا با TOE از خارج از محدودهTOE در تعامل است.

۳-۱-۳۴

خانواده

دسته‌بندی مؤلفه‌هایی که اهداف امنیتی را به اشتراک گذاشته اما در میزان اهمیت یا دقت با هم متفاوت باشند.

۳-۱-۳۵

رسمی

در زبان نحوی محدود شده با علم معنا شناسی تعیین شده که بر مبنای مفاهیم ریاضی تثبیت شده، توضیح داده می‌شود.

۳-۱-۳۶

اسناد راهنما

اسناد راهنما، تحویل، نصب، پیکربندی، عملیات، مدیریت و استفاده از هدف ارزیابی به عنوان فعالیت‌های به‌کارگرفته شده برای کاربران، مدیران و ایجاد کنندگان هدف ارزیابی را توضیح می‌دهد.

۳-۱-۳۷

هویت

معرفی هستاری که به طور خاص شناسایی شده است(برای مثال:یک کاربر،یک فرآیند یا یک دیسک)در حوزه تعریف TOE

یادآوری- مثال برای اینگونه نمایش یک رشته است.برای کاربر انسانی میتواند اسم کامل یا مختصر شده باشد(که هنوز یکتا است) یا یک تخلص.

1 -External IT entity

۳۸-۱-۳

غیر رسمی

با زبان طبیعی توضیح داده می‌شود.

۳۹-۱-۳

انتقالات TSF داخلی

مخابره داده‌ها میان TOE و عملیات امنیتی سایر محصولات فناوری اطلاعات مورد اطمینان.

۴۰-۱-۳

کانال ارتباطی داخلی

کانال ارتباطی میان قسمت‌های مختلف هدف ارزیابی می‌باشد.

۴۱-۱-۳

انتقال داخلی TOE

مخابره داده بین قسمتهای مجزای TOE

۴۲-۱-۳

سازگار به طور داخلی

هیچ گونه تناقضات آشکار بین هر جنبه از هستار وجود ندارد.

یادآوری- در شرایط استفاده از اسناد ، به این معنی است که نمی تواند هیچ گونه اظهاراتی در اسناد و مدارک که یکدیگر را نقض کند، وجود داشته باشد.

۴۳-۱-۳

تکرار

منظور استفاده از یک مؤلفه بیش از یک بار با عملیات متفاوت است.

۴۴-۱-۳

تطابق[1]

تجزیه و تحلیل منجر به نتیجه گیری

یادآوری- «تطابق» جدی تر از یک استدلال است. این اصطلاح نیاز به دقت قابل توجهی به لحاظ دقت زیاد طور کامل توضیح هر مرحله از استدلال منطقی است.

۴۵-۱-۳

موضوع

هستاری در درون TOE که در بر گیرنده یا دریافت‌کننده اطلاعات بوده و هستاری که موضوعات بر مبنای آن، عملیات را انجام می دهند.

۴۶-۱-۳

عمل

< بر روی یک مولفه از ISO/IEC 15408> اصلاح یا تکرار یک مولفه می‌باشد.

---

1 -Justification

یادآوری- عملیات مجاز بر روی مولفه‌ها، تغییر، تکرار، اصلاح و انتخاب است.

۳-۱-۴۷

عمل

<بر روی شی> نوع خاص از اقدام که به وسیله یک موضوع بر روی یک شئ انجام می‌شود

۳-۱-۴۸

محیط عملیاتی

محیطی که در آنTOE عمل می‌کند.

۳-۱-۴۹

خط‌مشی امنیت سازمانی

مجموعه‌ای از قواعد، رویه‌ها، یا رهنمودها برای یک سازمان

یادآوری- یک سیاست ممکن است به یک محیط عملیاتی خاص مربوط باشد.

۳-۱-۵۰

بسته

نام مجموعه ای از هر دو کارکرد یا نیازمندی های امنیتی تضمین

یادآوری- یک مثال برای بسته EAL3 است.

۳-۱-۵۱

ارزیابی رخ‌نمون محافظتی

ارزیابی یک PP در مقابل معیارهای تعریف شده.

۳-۱-۵۲

پروفایل محافظتی (PP)

یک‌سری الزامات امنیتی با پیاده سازی مستقل برای نوعی از .TOE

۳-۱-۵۳

ثابت کردن

نمایش تطابق با تجزیه و تحلیل رسمی در معنای ریاضی آن را نمایش می‌دهد.

یادآوری- این کاملا در تمام جهات دقیق است. به طور معمول، "اثبات" زمانی که تمایل به نشان دادن تطابق بین دو بازنمایی TSF در سطح بالایی از دقت وجود دارد استفاده می‌شود.

۳-۱-۵۴

پالایش[1]

اضافه نمودن جزئیاتی به مؤلفه می‌باشد.

1- refinement

۵۵-۱-۳

وظیفه

مجموعه قواعد از پیش تعیین شده که، تعامل‌های مجازی را میان کاربر و هدف ارزیابی (TOE) ایجاد می‌کند.

۵۶-۱-۳

رمز

اطلاعاتی که باید از آنها جهت مجاز نمودن کاربران و یا TSF در جهت اعمال‌نمودن SFPخاص، مطلع بود.

۵۷-۱-۳

حالت امن

حالتی که در آن داده TSF سازگاراست و TSF اجرای صحیح SFRs ادامه می‌دهد.

۵۸-۱-۳

ویژگی امنیتی

خصوصیات موضوعات، کاربران(شامل محصولات بیرونی IT)، اهداف، اطلاعات، و یا منابعی که جهت تعریف SFRs استفاده می شود و ارزش های آنها در اجرای SFRs به کار می‌رود.

۵۹-۱-۳

خط‌مشی عملیات امنیتی

مجموعه ای از قواعدی که رفتار امنیتی خاص به اجرا گذاشته شده توسط TSF و قابل بیان به عنوان یک مجموعه ای از SFRs را توصیف می‌کند.

۶۰-۱-۳

هدف امنیتی

بیان هدف از مقابله با تهدیدهای شناخته شده و/ یا اعمال نمودن خط‌مشی‌ها و فرضیات امنیتی سازمان می‌باشد.

۶۱-۱-۳

مشکل امنیتی

بیانیه ای که به شیوه ای رسمی ماهیت و حوزه امنیتی که برای پرداختن به TOE ، در نظر گرفته شده را، تعریف می‌کند

یادآوری- این بیانیه از ترکیبات زیر تشکیل شده است:

– تهدیدات برای مقابله با TOE

– OSPs به اجرا گذاشته توسط TOE، و

– مفروضاتی که برای TOEو محیط عملیاتی آن تایید شده است.

۶۲-۱-۳

الزامات امنیتی

الزامات، بیان شده در یک زبان استاندارد ، که به معنی کمک به دستیابی به اهداف امنیت برای TOE است.

۶۳-۱-۳

هدف امنیتی (ST)

یک سری از الزامات و مشخصه‌های امنیتی به کار رفته جهت ارزیابی TOE شناسایی شده می‌باشد.

۶۴-۱-۳

انتخاب

مشخصات یک یا تعداد بیشتری از اقلام از فهرستی از یک مؤلفه را انتخاب می‌نامند.

۶۵-۱-۳

نیمه رسمی[1]

با استفاده از زبان نحوی محدود با معانی تعیین شده، بیان می‌شود.

۶۶-۱-۳

مشخص کردن

ارائه جزئیات خاص در مورد هستار به شیوه ای جدی و دقیق

۶۷-۱-۳

انطباق دقیق

رابطه سلسله مراتبی بین PP و ST که در آن تمام الزامات مورد نیاز در PP در ST نیز وجود دارد

یادآوری- این رابطه را می‌توان تقریبا به عنوان «ST باید تمام اظهارات که درPP وجود دارد را داشته باشد، اما ممکن است شامل بیشتر از آن نیز باشد» شود. انتظار می‌رود مطابقت دقیق برای الزامات سختگیرانه که در یک حالت منفرد رعایت شده اند، اجرا شود.

۶۸-۱-۳

ارزیابی ST

ارزیابی یک ST در برابر معیارهای تعریف شده

۶۹-۱-۳

موضوع

هستار فعال در یک TOE که عملیات بر روی یک شی را انجام میدهد.

۷۰-۱-۳

هدف امنیتی

مجموعه ای از نرم افزار، میان افزار و/یا سخت افزار که احتمالا همراه با یک راهنما میابشد

۷۱-۱-۳

عامل تهدید

هستاری که میتواند به طور مخالف با یک دارایی عمل کند.

---

1 -semiformal

۷۲-۱-۳

ارزیابی TOE

ارزیابی TOEدر مقابل معیارهای تعریف شده.

۷۳-۱-۳

منبع هدف ارزیابی (TOE)

هر چیزی قابل مصرف و قابل استفاده در TOEرا منبع هدف ارزیابی می‌نامند.

۷۴-۱-۳

عملکرد امنیتی TOE

عملکرد ترکیبی از تمام سخت افزار، نرم افزار و میان افزار TOE است که باید بر اجرای صحیح SFRs متکی باشد.

۷۵-۱-۳

ردیابی، فعل

ردیابی، فعل

انجام تجزیه و تحلیل مطابقت غیر رسمی بین دو هستار با تنها کمترین سطح دقت

۷۶-۱-۳

نقل و انتقالات خارج از TOE

ارتباطات میانی TSF از داده به هستارها تحت کنترل TSF.

۷۷-۱-۳

ترجمه

توصیف فرآیندتشریح نیازمندی‌های امنیتی در یک زبان استاندارد

یادآوری- استفاده از لغت ترجمه در این زمینه تحت اللفظی نیست و بدان معنا نیست که هر SFR بیان شده در زبان استاندارد نیز می‌تواند به اهداف امنیتی ترجمه شود.

۷۸-۱-۳

کانال مطمئن

ابزاری که یک TSF و محصول فناوری اطلاعات مطمئن از راه دور می‌تواند ، با اطمینان کافی، با آن ارتباط برقرار کند.

۷۹-۱-۳

محصول قابل اعتماد IT

محصول IT ، متفاوت از TOE، که دارای الزامات عملکردی امنیتی خود که از نظر اجرایی هماهنگ شده با TOE می‌باشد و فرض شده است که الزامات عملکرد امنیتی خود را به درستی اجرا می‌کند.

یادآوری- به عنوان مثال از محصول مورد اعتماد IT محصولی خواهد بودکه به طور جداگانه مورد بررسی قرار گرفته است.

۳-۱-۸۰

روش مطمئن

ابزاری که کاربر و TSF می‌تواند با اطمینان کامل با آن ارتباط برقرار کند.

۳-۱-۸۱

داده TSF

داده برای عملیات TOE که اجرای SFR بر اساس آن متکی است.

۳-۱-۸۲

رابط TSF

بدان معنی است که از طریق آن هستارهای خارجی (یا موضوعات در TOE، اما در خارج از TSF) داده را برای TSF،تامین می‌کنند، اطلاعات را از TSF دریافت میکنند و خدمات را از TSF فراخوانی می‌کنند.

۳-۱-۸۳

داده‌های کاربری

داده‌ای برای کاربر که بر روی عملکرد TSF تاثیر نمی‌گذارد.

۳-۱-۸۴

تأیید

مرور دقیق با جزئیات با اراده کافی مستقل

یادآوری- همچنین "تایید" (به بند ۳-۱-۱٤مراجعه کنید).اصطلاح "تایید" دارای معانی دقیق است. در زمینه اقدامات ارزیاب که در آن تلاش مستقل ارزیاب لازم است، مورد استفاده قرار می‌گیرد.

۳-۲ اصطلاحات و تعاریف مربوط به گروه ADV

یادآوری- شرایط و ضوابط ذیل در الزامات مورد نیاز برای ساختار نرم افزار داخلی مورد استفاده قرار می‌گیرند. برخی از این از IEEE STD 610.12-1990 مشتق شده است، واژه نامه استاندارد اصطلاحات مهندسی نرم افزار، موسسه برق و مهندسین الکترونیک

۳-۱-۲

مدیر

هستاری که یک سطح اعتماد را با توجه به تمام سیاست‌های اجرا شده توسط TSF داراست.

یادآوری- تمام PPها یا STها سطح یکسانی از اعتماد برای مدیران را فرض نمیکنند. به طور معمول فرض میشود مدیران در تمامی زمان‌ها بر پایبندی به سیاست‌های ST از TOE مقید هستند. برخی از این سیاست‌ها ممکن است مربوط به عملکرد TOE، و برخی دیگر ممکن است مربوط به محیط عملیاتی باشد.

۳-۲-۲

درخت فراخوانی

برای شناسایی پودمان‌ها در یک سامانه در قالب خطوط هندسی که نشان میدهد کدام پودمانها یکدیگر را فراخوانی میکنند

یادآوری اقتباس از IEEE STD 610.12-1990.

۳-۲-۳

پیوستگی

قدرت پودمان

شیوه و درجه ای که کارهای انجام شده توسط یک پودمان نرم افزار را به یکدیگر مرتبط می‌کند

[IEEE STD 610.12-1990]

یادآوری- انواع انسجام شامل تصادفی، ارتباطی، تابعی، منطقی، متوالی، و زمانی است. این انواع از انسجام به وسیله ورودی اصطلاح مربوطه شرح داده شده است.

۴-۲-۳

انسجام تصادفی

پودمان همراه با ویژگی‌های فعالیتهای نامربوط انجام شده، و یا ربط خیلی کمرنگ،

[IEEE STD 610.12-1990]

یادآوری- همچنین انسجام (به بند ۳-۲-۲ مراجعه کنید) را ببینید.

۵-۲-۳

انسجام ارتباطی

پودمان حاوی توابع است که خروجی برای، و یا استفاده از خروجی، توابع دیگر در داخل پودمان را تولید می‌کند

[IEEE STD 610.12-1990]

یادآوری ۱- همچنین انسجام (به بند ۳-۲-۲ مراجعه کنید) را ببینید.

یادآوری ۲- نمونه ای از یک پودمان ارتباطی منسجم ،یک پودمان چک دسترسی است که شامل اجباری اختیاری، و چکهای قابلیت میباشد

۶-۲-۳

پیچیدگی

اندازه گیری این موضوع که تا چه حد نرم افزار فهم نرم افزار مشکل است، وبنابراین تجزیه و تحلیل، تست، و حفظ آن تا چه حد مشکل است

[IEEE STD 610.12-1990]

یادآوری- کاهش پیچیدگی هدف نهایی با استفاده از تجزیه مدولار، لایه بندی و کمینه سازی است.کنترل جفت و انسجام کمک قابل توجهی به این هدف است.

تلاش خوبی در زمینه مهندسی نرم افزار برای توسعه معیارهای پیچیدگی کد منبع انجام شده است. بسیاری از این معیارها به راحتی از خواص قابل محاسبه کد منبع، مانند تعداد اپراتورها و عملوندها، پیچیدگی نمودار کنترل جریان (پیچیدگی)، تعداد خطوط کد منبع، نسبت پیشنهادات به کد اجرایی، و اقدامات مشابه، استفاده میکنند. برنامه نویسی استاندارد شده یافت شده‌اند که ابزار مفیدی در تولید کدهایی که به آسانی قابل درک هستند، می‌باشد.

خانواده TSF داخلی(ADV_INT) خواستار تجزیه و تحلیل پیچیدگی در تمام مولفه‌ها می‌باشد. انتظار می‌رود که توسعه دهنده، پشتیبانی برای ادعاهایی که کاهش کافی در پیچیدگی وجود دارد را فراهم خواهد کرد. این حمایت می‌تواند شامل استانداردهای برنامه نویسی توسعه دهنده ، نشان دهنده این که تمام پودمانها با استاندارد منطبق هستند(یا این که برخی از استثناها که توسط استدلال‌های مهندسی نرم افزار توجیه شده) باشد. همچنین می‌تواند شامل نتایج حاصل از ابزارهای مورد استفاده برای اندازه گیری برخی از خواص کد منبع، یا حمایت‌های دیگری که توسعه دهنده انجام میدهد، مناسب باشد.

۳-۲-۷

اتصال[1]

نحوه و میزان وابستگی بین پودمان‌های نرم افزار

[IEEE STD 610.12-1990]

یادآوری-انواع اتصال شامل تماس، اشترک و اتصال محتوا. اینها در زیر مشخص شده اند.

۳-۲-۸

اتصال فراخوانی

ارتباط بین دو پودمان که اکیدا ارتباط برقرار کرده اند از طریق فراخوانی تابع مستند شده آن تابعها

یادآوری- مثالهایی از اتصال، فراخوانی داده، تمبر و کنترل است.

۳-۲-۹

اتصال فراخوانی

<داده> ارتباط بین دو پودمان که اکیدا ارتباط برقرار کرده اند از طریق استفاده از پارامترهای فراخوانی که انواع داده منفرد را نشان میدهد.

یادآوری- همچنین اتصال فراخوانی را ببینید (به بند ۳-۲-۸ مراجعه شود).

۳-۲-۱۰

اتصال فراخوانی

<استمپ> رابطه بین دو پودمان که از طریق استفاده از پارامترهای فراخوانی که شامل زمینه‌های مختلف و یا ساختار داخلی معنی دار هستند ارتباط برقرار می‌کنند.

یادآوری- همچنین اتصال فراخوانی را ببینید (۳-۲-۸).

1- coupling

۱۱-۲-۳

اتصال فراخوانی

<کنترل> ارتباط بین دو پودمان اگر یکی اطلاعات در نظر گرفته شده برای نفوذ در منطق درونی دیگر را عبور دهد.

یادآوری- همچنین اتصال فراخوانی را ببینید (۳-۲-۸).

۱۲-۲-۳

اتصال مشترک

ارتباط بین دو پودمان که منطقه داده مشترک و یا دیگر منابع سامانه مشترک را به اشتراک می‌گذارند.

یادآوری- متغیرهای سراسری نشان می‌دهد که پودمانهایی که از این متغیرهای سراسری استفاده می‌کنند اتصال مشترک هستند. اتصال مشترک که به طور کلی از طریق متغیرهای سراسری است مجاز است، اما تنها به یک درجه برای مثال، متغیرهایی که در یک منطقه سراسری قرار گرفته اند، اما تنها با یک پودمان استفاده می‌شوند، در جای نادرستی قرار گرفته‌اند و باید برداشته شوند. عوامل دیگری که نیاز است درنظر گرفته شوند برای ارزیابی مناسب از متغیرهای سراسری عبارتند از:

تعدادی از پودمان‌هایی که یک متغیر سراسری را تغییرمی‌دهند: به طور کلی، تنها یک پودمان باید به عنوان مسئول کنترل محتویات یک متغیر سراسری اختصاص داده شود ، اما ممکن است در موقعیتهایی که در آن یک پودمان دوم آن مسئولیت را به اشتراک بگذارد ، در چنین مواردی، توجیه کافی باید بیان شود. این که این مسئولیت بین بیش از دو پودمان به اشتراک گذاشته شود غیر قابل قبول است. (در این ارزیابی، توجه کافی باید صرف پودمانی که مسئول محتوای متغیر است شود.

به عنوان مثال، اگر روال منفردی برای تغییر متغیر استفاده شده است، اما این روال به سادگی اصلاح درخواست شده توسط تماس گیرنده خود را انجام می‌دهد ، این پودمان فراخوانی است که مسئول است، و ممکن است بیش از یک چنین پودمانی وجود داشته باشد). علاوه بر این، به عنوان قسمتی از تعیین پیچیدگی، اگر دو پودمان مسئول محتویات یک متغیر سراسری هستند، باید نشانه‌های روشنی از این که چگونه تغییرات بین آنها هماهنگ شده است وجود داشته باشد.

تعدادی از پودمان‌ها که مرجع یک متغیر سراسری هستند، هر چند به طور کلی هیچ محدودیتی در تعداد پودمان‌های که مرجع یک متغیر سراسری هستند وجود ندارد، مواردی که در آن بسیاری از پودمان‌ها از جمله مرجع باید برای اعتبار و ضرورت بررسی شوند وجود دارد.

۱۳-۲-۳

اتصال محتوا

ارتباط بین دو پودمان که یکی از آنها اشاره مستقیمی به ورودی‌های دیگری ایجاد می‌کند.

یادآوری-برای مثال تغییر کد و یا ارجاع برچسب داخلی، به پودمان دیگر. نتیجه این است که همه یا برخی از محتوای یکی از پودمان‌ها به طور موثر شامل دیگری نیز می‌شود. اتصال محتوا می‌تواند با استفاده از واسطهای پودمان مبهم در نظر گرفته شود. این موضوع در تضاد با اتصال فراخوانی است، که فقط از واسطهای پودمان عمومی استفاده می‌کند.

۱۴-۲-۳

جدایی دامنه

ویژگی معماری امنیتی است که در آن TSF حوزه‌های امنیتی جداگانه برای هر کاربر و برای TSF را تعریف می‌کند و تضمین می‌کند که هیچ کاربر نتواند محتویات را از دامنه امنیتی از کاربر دیگری و یا TSF تحت تاثیر قرار دهد.

۱۵-۲-۳

انسجام عملکردی

ویژگی عملکردی از یک پودمان است که فعالیت‌های مربوط به یک هدف واحد را انجام می‌دهد.
[IEEE STD 610.12-1990]

یادآوری- یک پودمان عملکرد منسجم که یک نوع ورودی را به یک نوع خروجی تبدیل می‌کند ، مانند یک پشته مدیر و یا یک مدیر صف. همچنین انسجام را ببینید (به بند ۳-۲-۳ مراجعه کنید.).

۱۶-۲-۳

بر هم کنش

ارتباطات مبتنی بر فعالیت عمومی بین هستارها

۱۷-۲-۳

رابط

به معنی بر هم کنش با یک مولفه یا پودمان

۱۸-۲-۳

لایه بندی

روش طراحی که در آن گروه‌های جداگانه ای از پودمان‌ها (لایه‌ها) به صورت سلسله مراتبی برای داشتن مسئولیت‌های جداگانه سازماندهی شده‌اند به طوری که یک لایه تنها بر لایه‌های زیر آن را در سلسله مراتب خدمات وابسته است، و خدمات خود را فقط برای لایه‌های بالای آن فراهم می‌کند.

یادآوری- لایه بندی اکید اضافه می‌کند که محدودیت هر لایه خدمات را تنها از لایه بلافاصله زیر آن دریافت می‌کند، و خدمات را تنها به لایه بلافاصله بالاتر از آن ارائه می‌کند.

۱۹-۲-۳

انسجام منطقی

انسجام رویه

خصوصیات یک پودمان در انجام فعالیت‌های مشابه بر روی ساختمان داده‌های مختلف

یادآوری- یک پودمان انسجام منطقی را در صورتی که انجام توابع به آن مربوط باشد نشان می‌دهد ، اما متفاوت از، عملیات بر روی ورودی‌های مختلف

همچنین انسجام را ببینید (به بند ۳-۲-۳ مراجعه کنید.)

۲۰-۲-۳

تجزیه مدولار

فرآیند شکستن یک سامانه به اجزای سازنده برای تسهیل طراحی، توسعه و ارزیابی
[IEEE STD 610.12-1990]

۲۱-۲-۳

بدون bypassability

<برای TSF > اموال معماری امنیت که به موجب آن تمام عملیات مربوط به SFR به واسطه TSF انجام می‌پذیرد

۲۲-۲-۳

امنیت دامنه

مجموعه ای از منابع که یک هستار فعال دارای مزایای دسترسی به آنها است.

۲۳-۲-۳

انسجام ترتیبی

پودمان شامل توابعی که خروجی هر کدام از آنها ورودی برای تابع زیر در پودمان است.
[IEEE STD 610.12-1990]

یادآوری –یک مثال از پودمان ترتیبی منسجم، نوعی است که شامل توابع به منظور نوشتن سوابق ممیزی و حفظ یک تعداد شماره‌های تجمع نقض ممیزی در حال اجرا از نوع به خصوص می‌باشد.

۲۴-۲-۳

مهندسی نرم افزار

استفاده از یک رویکرد سامانهاتیک، منظم، قابل سنجش به منظور توسعه و نگهداری نرم افزار ،که این، کاربرد مهندسی در نرم افزار است.
[IEEE STD 610.12-1990]

یادآوری -همانطور که با شیوه‌های فنی و مهندسی به طور کلی، مقداری توجیه باید در استفاده از اصول مهندسی استفاده می‌شود. بسیاری از عوامل بر انتخابها اثر می‌گذارند ، نه فقط با استفاده از اقدامات تجزیه مدولار، لایه بندی، و کمینه ساختن. به عنوان مثال، توسعه دهنده ممکن است یک سامانه را با برنامه‌های آینده در ذهن که در ابتدا اجرا نمی شود طراحی کند. توسعه دهنده ممکن است برخی از منطقها را که شامل مسئولیت رسیدگی به این برنامه‌های آینده می‌باشد، انتخاب کند بدون این که به طور کامل آنها را پیاده سازی کند، علاوه بر این، توسعه دهنده ممکن است برخی از فراخوانی‌ها که هنوز پودمان‌های اجرا نشده هستند را نیز شامل شود. توجیه توسع دهنده برای انحراف‌های این چنینی از برنامه‌هایی با ساختار خوب باید با قضاوت ارزیابی شوند، همانطور برنامه کاربردی نظم مهندسی نرم افزار خوب.

۲۵-۲-۳

انسجام زمانی

ویژگی‌های یک پودمان شامل توابعی که نیاز است تقریبا در یک زمان مشابه اجرا شوند.

یادآوری ۱- از [IEEE STD 610.12-1990] اقتباس شده است.

یادآوری ۲- نمونه از پودمان‌های موقتا منسجم که عبارتند از مقدار دهی اولیه، بهبود، و پودمان‌های خاموش کردن سامانه.

۲۶-۲-۳

حفاظت از خود TSF

۳-۳ اصطلاحات و تعاریف مربوط به گروه AGD

۱-۳-۳

نصب

رویه انجام شده توسط یک کاربر انسانی که TOE را در محیط عملیاتی خود تعبیه می‌کند و آن را به حالت عملیاتی قرار می‌هد.

یادآوری- این عمل به طور معمول تنها یک بار، پس از دریافت و پذیرش TOE انجام شده است. انتظار می‌رود TOE به پیکربندی که توسط ST اجازه داده شده، توسعه یابد. اگر فرآیندهای مشابه توسط توسعه‌دهنده باید انجام شود آنها به عنوان "تولید" در سراسر ALC استفاده می‌شود: حمایت از چرخه زندگی. اگر TOE نیاز به راه اندازی اولیه که لازم نیست به طور منظم تکرار شود، داشته باشد، این روند می‌تواند به عنوان نصب و راه اندازی طبقه بندی می‌شود.

۲-۳-۳

عمل

مرحله کاربرد TOE شامل «کاربرد طبیعی»، مدیریت و نگهداری از TOE بعد از تحویل و آماده سازی.

۳-۳-۳

آماده سازی

فعالیت در مرحله چرخه عمر یک محصول، شامل پذیرش مشتری از TOE تحویل داده شده و نصب و راه اندازی آن که ممکن است شامل چیزهایی مانند بوت شدن، مقدار دهی اولیه، راه اندازی و پیشرفت TOEبه حالت آماده برای عمل باشد.

۴-۳ اصطلاحات و تعاریف مربوط به کلاس ALC

۱-۴-۳

معیارهای پذیرش

معیارهای به کار گرفته شده در هنگام اجرای مراحل پذیرش (به عنوان مثال بررسی سند موفقیت آمیز باشد، و یا آزمون موفقیت آمیز در مورد نرم افزار، سامانه عامل یا سخت افزار)

۲-۴-۳

روال‌های پذیرش

روال‌های دنبال شده به منظور پذیرفتن اقلامی که تازه ایجاد شده و یا تغییر پیکربندی شده‌اند به عنوان قسمتی از TOE، و یا انتقال آنها به مرحله بعدی چرخه زندگی

یادآوری- این روال‌ها نقش‌ها و یا مسئولیت افراد برای پذیرش و معیارهای به کار گرفته شده به منظور تصمیم گیری در پذیرش را شناسایی می‌کنند.

انواع مختلفی از شرایط پذیرش که بعضی از آنها ممکن است با هم تداخل داشته باشند، وجود دارد:

الف- پذیرش یک آیتم به مدیریت پیکربندی سامانه برای اولین بار، در گنجاندن به خصوصی از نرم افزار، میان‌افزار و مولفه‌های سخت افزار از دیگر تولید کنندگان به TOE («ادغام»)؛

ب) توسعه اقلام پیکربندی به مرحله بعدی چرخه زندگی در هر مرحله از ساخت و ساز TOE(برای مثال روال، زیر سامانه، کنترل کیفی TOE به اتمام رسیده)؛

ج) در ادامه برای حمل و نقل از اقلام پیکربندی (برای نمونه قطعاتی از TOEیا محصولات مقدماتی) بین سایت‌های متفاوت توسعه؛

د) پس از آن تحویل TOE به مصرف کننده می‌باشد.

۳-۴-۳

مدیریت پیکربندی

CM

نظم و انضباط در استفاده از جهت و نظارت فنی و اداری برای شناسایی و مستندسازی خصوصیات عملکردی و فیزیکی از قلم دوم از اقلام پیکربندی، تغییرات کنترل به آن دسته از خصوصیات، ثبت و گزارش پردازش و تغییر وضعیت پیاده سازی و بررسی انطباق با الزامات مشخص شده است.

یادآوری- اقتباس از استاندارد IEEE 610.12 است.

۴-۴-۳

مستندات CM

همه اسناد CM از جمله خروجی CM، فهرست CM (فهرست پیکربندی)، رکوردهای سامانه CM ، طرح CM و استفاده از اسناد و مدارک CM می‌باشد.

۵-۴-۳

مدیریت پیکربندی شواهد

هر آنچه را که ممکن است مورد استفاده قرار گیرد برای ایجاد اعتماد به نفس در عملکرد صحیح سامانه CM.

یادآوری- به عنوان مثال، خروجی CM، دلایل ارائه شده توسط توسعه دهنده، مشاهدات، آزمایشات و یا مصاحبه توسط ارزیاب در طی ساخت یک سایت.

۶-٤-۳

آیتم پیکربندی

شیء مدیریت شده توسط سامانه CM

یادآوری- این ممکن است یا قسمت‌هایی از TOEو یا اشیاء مربوط به توسعه TOE مانند اسناد ارزیابی و یا ابزارهای توسعه. اقلام CM ممکن است در سامانه CM به طور مستقیم (به عنوان مثال، فایلها) و یا مرجع (به عنوان مثال قطعات سخت افزاری) به همراه نسخه خود ذخیره شوند.

۷-۴-۳

فهرست پیکربندی

مدیریت پیکربندی سند خروجی تمام اقلام پیکربندی برای یک محصول خاص به همراه نسخه دقیق هر یک از اقلام مدیریت پیکربندی مربوط به یک نسخه خاص از محصول کامل را فهرست می‌کند.

یادآوری- این فهرست تشخیص اقلام متعلق به نسخه ارزیابی محصول از نسخه‌های دیگر از این موارد متعلق به نسخه‌های دیگر از این محصول را فراهم می‌کند. فهرست مدیریت پیکربندی نهایی یک سند خاص برای یک نسخه خاص از یک محصول خاص می‌باشد. (البته این فهرست می‌تواند یک سند الکترونیکی در داخل یک ابزار مدیریت پیکربندی باشد در آن صورت می‌توان آن را به عنوان یک نگاه خاص به سامانه یا قسمتی از سامانه به جای خروجی از سامانه دید. با این حال، برای استفاده عملی در ارزیابی فهرست پیکربندی احتمالا به عنوان یک قسمتی از اسناد ارزیابی تحویل داده شود.) فهرست پیکربندی اقلامی که تحت نیازمندی‌های مدیریت پیکربندی ALC_CMC هستند را تعریف می‌کند.

۸-۴-۳

خروجی مدیریت پیکربندی

نتایج مربوط به مدیریت پیکربندی، تولید و اجرا توسط سامانه مدیریت پیکربندی

یادآوری- این نتایج مربوط به مدیریت پیکربندی می‌تواند به عنوان اسناد در نظر گرفته شود (به عنوان مثال فرم‌های کاغذی پر شده، پیکربندی سامانه مدیریت مدارک، اطلاعات ورود به سامانه، نسخه چاپی و داده‌های خروجی الکترونیکی) و همچنین عملیات (برای مثال کتابچه راهنمای کاربر تکمیل دستورالعمل‌های مدیریت پیکربندی را اندازه‌گیری می‌کند). نمونه‌هایی از چنین خروجی مدیریت پیکربندی فهرست‌های پیکربندی هستند، برنامه‌های مدیریت پیکربندی و / یا رفتارهای در طول چرخه عمر محصول می‌باشند.

۹-۴-۳

برنامه مدیریت پیکربندی

توضیحات در مورد چگونگی سامانه مدیریت پیکربندی برای TOE مورد استفاده قرار می‌گیرد

یادآوری- هدف از انتشار طرح مدیریت پیکربندی این است که کارمندان به وضوح می‌توانند ببینند چه کاری را باید انجام دهند. از نقطه نظر سامانه مدیریت پیکربندی کلی این را می‌توان به عنوان سند خروجی (زیرا ممکن است به عنوان قسمتی از کاربرد سامانه مدیریت پیکربندی معرفی شود) دید. از نقطه نظر پروژه مهم و اساسی یک سند قابل استفاده است، چرا که اعضای تیم پروژه از آن به منظور درک مراحلی که در طول پروژه مجبور به انجام آنها هستند، استفاده می‌کنند. طرح مدیریت پیکربندی، استفاده از سامانه برای محصول خاص را تعریف می‌کند، همان سامانه را می‌توان به اندازه‌های مختلف برای محصولات دیگر استفاده کرد. این بدان معناست که طرح مدیریت پیکربندی خروجی از سامانه مدیریت پیکربندی از یک شرکت که در طول توسعه TOE استفاده می‌شود، تعریف و توصیف می‌کند.

۱۰-۴-۳

سامانه مدیریت پیکربندی

مجموعه ای از روال‌ها و ابزارها (از جمله اسناد آنها) مورد استفاده توسط یک برنامه نویس برای توسعه و حفظ تنظیمات محصولاتشان در طول چرخه زندگی.

یادآوری- پیکربندی سامانه‌های مدیریت ممکن است درجات مختلفی از دقت و عملکرد را داشته باشند. در سطوح بالاتر، سامانه‌های مدیریت پیکربندی ممکن است خودکار با اصلاح نقص باشند، کنترل‌ها را تغییر دهد، و دیگری ساز و کار ردیابی شده است.

۱۱-۴-۳

سوابق سامانه مدیریت پیکربندی

خروجی تولید شده در طول عملیات سامانه مدیریت پیکربندی مستند سازی فعالیت‌های مهم مدیریت پیکربندی

یادآوری- نمونه‌هایی از پرونده‌های سامانه مدیریت پیکربندی ، مدیریت پیکربندی مورد تغییر فرم‌های کنترل یا مدیریت پیکربندی مورد دسترسی به فرم‌های تایید هستند

۱۲-۴-۳

ابزارهای مدیریت پیکربندی

ابزارهای دستی و یا خودکار در تحقق و یا حمایت از یک سامانه مدیریت پیکربندی است.

یادآوری- برای ابزار به عنوان مثال ابزار برای مدیریت نسخه قسمتهایی از TOE.

۱۳-۴-۳

مستند سازی استفاده از مدیریت پیکربندی

قسمتی از سامانه مدیریت پیکربندی است که توضیح می‌دهد چگونه سامانه مدیریت پیکربندی تعریف شده است و با استفاده از، برای مثال، کتابچه، مقررات و / یا ابزارهای مستندسازی و روال‌ها به کار گرفته می‌شود.

۱۴-۴-۳

تحویل

انتقال TOE به پایان رسیده از محیط تولید به دست مشتری را تحویل گویند.

یادآوری- این مرحله چرخه زندگی محصول ممکن است شامل بسته بندی و ذخیره سازی در توسعه سایت باشد، اما حمل و نقل TOE ناتمام و یا قسمت‌هایی از TOE در بین توسعه دهندگان مختلف و یا سایت‌های مختلف توسعه را شامل نمی شود.

۱۵-۴-۳

توسعه دهنده

سازمان مسئول برای توسعه TOE است.

۱۶-۴-۳

توسعه

مرحله چرخه زندگی محصول است که به ایجاد نمایش پیاده سازی TOE مربوط می‌شود.

یادآوری- در طول الزامات ALC، توسعه و اصطلاحات مربوط به (توسعه‌دهنده، توسعه) در معنای کلی تر شامل توسعه و تولید می‌شوند

۱۷-۴-۳

ابزارهای توسعه

ابزار (از جمله نرم افزار آزمون، در صورت قابل اجرا بودن) حمایت از توسعه و تولید TOE می‌باشد.

یادآوری- به عنوان مثال، برای نرم افزار TOE، ابزار توسعه معمولا از زبان‌های برنامه نویسی، کامپایلرها ، پیونددهنده‌ها و ابزارهای تولید تشکیل می‌شود.

۱۸-۴-۳

نمایش پیاده سازی

کمترین بازنمایی انتزاعی از TSF، به خصوص آن نوعی که برای ایجاد خود TSF بدون پالایش طراحی بیشتر استفاده می‌شود

یادآوری- کد منبعی که سپس کامپایل شده و یا طراحی سخت افزاری که برای ساخت سخت افزار واقعی استفاده می‌شود، نمونه‌هایی از قطعات نمایش پیاده سازی شده هستند.

۱۹-۴-۳

چرخه زندگی

دنباله ای از مراحل وجود یک شیء (برای مثال یک محصول و یا یک سامانه) در زمان

۲۰-۴-۳

تعریف چرخه زندگی

تعریف مدل چرخه زندگی است.

۲۱-۴-۳

مدل چرخه زندگی

شرح مراحل و ارتباط آنها به یکدیگر است که در مدیریت چرخه زندگی یک شی خاص استفاده می‌شود، چگونه دنباله ای از مراحل به نظر می‌رسند و مراحل کدام یک از خصویات سطح بالا را شامل می‌شوند.

یادآوری- همچنین شکل ۱را ببینید.

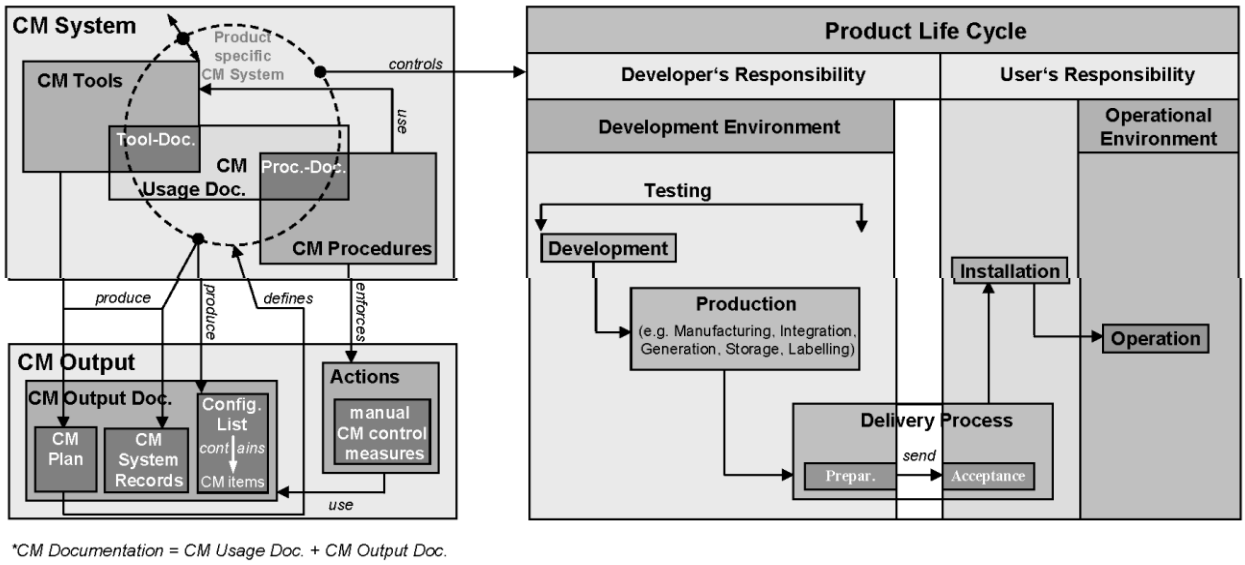
۲۲-۴-۳

تولید

تولید مرحله چرخه زندگی مرحله توسعه را دنبال می‌کند و متشکل از تبدیل نمایش پیاده سازی به پیاده سازی TOE است، یعنی به یک حالت قابل قبول برای تحویل به مشتری

یادآوری ۱- این مرحله ممکن است ساخت، یکپارچه سازی، تولید، حمل و نقل داخلی، ذخیره سازی، و برچسب زدن TOE را تشکیل دهد.

یادآوری ۲- همچنین شکل ۱را ببینید.



شکل۱-واژگان فنی در CM و چرخه حیات محصول

۳-۵ اصطلاحات و تعاریف مربوط به کلاس AVA

۱-۵-۳

کانال پنهان

اجرای، کانال سیگنال‌دهی غیرقانونی که اجازه نقض محرمانه سیاست جدایی چند سطحی و عدم مشاهده الزامات TOE را به کاربر می‌دهد.

۲-۵-۳

مواجه با آسیب پذیری‌های بالقوه

ضعف بالقوه شناسایی شده در TOE توسط ارزیاب هنگامی که فعالیت‌های ارزیابی را که می‌تواند مورد استفاده نقض SFRs قرار گیرد، انجام می‌دهد.

۳-۵-۳

آسیب پذیری قابل بهره برداری

ضعف TOE که می‌تواند مورد استفاده نقض SFRs در محیط عملیاتی برای TOE، قرار گیرد.

۴-۵-۳

حملات نظارت

دسته بندی کلی از روش‌های حمله که شامل فنون تجزیه و تحلیل غیرفعال با هدف افشای اطلاعات حساس داخلی TOE ، توسط راه اندازی TOE در راهی که مربوط به مستندات راهنما است، می‌باشد.

۵-۵-۳

آسیب پذیری بالقوه

مشکوک ، اما تایید نشده ، نقطه ضعف

۶-۵-۳

آسیب پذیری باقی مانده

نقطه ضعفی که نمی تواند در محیط عملیاتی برای TOE مورد سوء استفاده قرار گیرد، اما می‌تواند برای نقض SFRs به وسیله یک مهاجم، با پتانسیل حمله بیشتر از آن چیزی که در محیط عملیاتی برای TOE پیش بینی شده، استفاده شود.

۷-۵-۳

آسیب پذیری

نقطه ضعفی در TOE که می‌تواند برای نقض SFRs در برخی از محیط‌ها، مورد استفاده قرار گیرد.

۳-۶ اصطلاحات و تعاریف مربوط به کلاس ACO

۱-۶-۳

مولفه پایه

هستار در TOE مرکب، که خود موضوع ارزیابی شده است، خدمات و منابع برای یک مولفه وابسته را فراهم می‌کند.

۲-۶-۳

سازگار

<مولفه‌ها > ویژگی یک مولفه که قادر به ارائه خدمات مورد نیاز مولفه دیگر، از طریق رابط‌های مربوط به هر مؤلفه، در محیط‌های عملیاتی سازگار، است.

۳-۶-۳

مولفه TOE

ارزیابی موفقیت آمیز TOE که قسمتی از یک TOE مرکب دیگر است.

۴-۶-۳

TOE مرکب

TOE که فقط از دو یا بیشتر از دو مولفه که با موفقیت مورد بررسی قرار گرفته‌اند، تشکیل شده است.

۵-۶-۳

مولفه وابسته

هستار در یک TOEمرکب، که خود این موضوع یک ارزیابی است، با تکیه بر خدمات ارائه شده توسط مولفه پایه.

۶-۶-۳

رابط کاربری عملکردی

رابط خارجی، یک کاربر با دسترسی به قابلیت‌های TOE ارائه می‌کند که به طور مستقیم درگیر اجرای نیازمندی‌های تابعی امنیتی نمی‌باشد.

یادآوری-در یک TOE مرکب این‌ها رابط‌های ارائه شده توسط مولفه پایه هستند که لازم است توسط مولفه وابسته برای حمایت از عملیاتTOEمرکب استفاده شوند.

۴ اصطلاحات مختصر شده

اختصارات زیر در یک یا چند قسمت از این استاندارد ملی مورد استفاده قرار می‌گیرند.

API	Application Programming Interface	واسط برنامه نویسی کاربردی
CAP	Composed Assurance Package	بسته تضمین مرکب
CM	Configuration Management	مدیریت پیکربندی
DAC	Discretionary AISO/IEC 15408ess Control	کنترل دسترسی اختیاری
EAL	Evaluation Assurance Level	سطح تضمین ارزیابی
GHz	Gigahertz	گیگاهرتز
GUI	Graphical User Interface	واسط کاربری نگاره‌ای
IC	Integrated Circuit	مدار مجتمع
IOCTL	Input Output Control	کنترل ورودی خروجی
IP	Internet Protocol	پروتکل اینترنت
IT	Information Technology	فناوری اطلاعات
MB	Mega Byte	مگا بایت
OS	Operating System	سامانه عامل
OSP	Organizational Security Policy	سیاست امنیتی سازمانی
PC	Personal Computer	رایانه شخصی
PCI	Peripheral Component Interconnect	اتصال مولفه‌های محیطی
PKI	Public Key Infrastructure	زیرساخت کلید عمومی
PP	Protection Profile	رخ‌نمون محافظتی
RAM	Random AISO/IEC 15408ess Memory	حافظه با دسترسی تصادفی
RPC	Remote Procedure Call	فراخوانی پردازه از راه دور
SAR	Security Assurance Requirement	نیازمندی‌های تضمین امنیت
SFR	Security Functional Requirement	نیازمندی‌های عملیاتی امنیت
SFP	Security Function Policy	سیاست عملیاتی امنیت

SPD	Security Problem Definition	تعریف مشکل امنیتی
ST	Security Target	هدف امنیتی
OSP	Organizational Security Policy	سیاست امنیتی سازمانی
TCP	Transmission Control Protocol	پروتکل کنترل انتقال
TOE	Target of Evaluation	هدف امنیتی
TSF	TOE Security Functionality	عملیات امنیتی TOE
TSFI	TSF Interface	واسط TSF
VPN	Virtual Private Network	شبکه خصوصی مجازی

۵ مرور کلی

۵-۱ عمومی

این بند مفاهیم اصلی این استاندارد ملی را معرفی می‌کند.این بند مفهوم «TOE » ، مخاطبان هدف ISO / IEC 15،408، و رویکرد گرفته شده برای ارائه مواد باقی مانده از این استاندارد ملی را مشخص می‌کند.

۵-۲ TOE

این استاندارد ملی در این مورد که چه چیزی ارزیابی شود انعطاف پذیر است و بنابراین به محدوده محصولات IT آن طوری که معمولا قابل درک است تعلق ندارد. بنابراین در زمینه ارزیابی، این استاندارد ملی از اصطلاح "TOE" (هدف امنیتی) استفاده می‌کند.

TOE، به عنوان مجموعه ای از نرم افزار، میان‌افزار و / یا سخت افزار احتمالا همراه با راهنما، تعریف شده است.

در حالی که مواردی که در آن یک TOE متشکل از یک محصول IT است، وجود دارد، این مورد لازم نیست. TOE ممکن است یک محصول IT، قسمتی از یک محصولIT ، مجموعه ای از محصولات فناوری اطلاعات، تکنولوژی منحصر به فردی که ممکن است هرگز در یک محصول به کار نرفته باشد، و یا ترکیبی از این موارد است.

تا آنجا که به این استاندارد ملی مربوط است، رابطه دقیق بین TOE و هر نوعی از محصولات IT تنها در یک جنبه اهمیت دارد: ارزیابی TOE حاوی تنها قسمتی از یک محصول IT نباید به عنوان ارزیابی تمام محصول به صورت نادرست ارایه شود.

نمونه‌هایی از TOE عبارتند از:

- نرم افزار کاربردی؛
- یک سامانه عامل؛
- یک نرم افزار کاربردی در ترکیب با یک سامانه عامل؛
- یک نرم افزار کاربردی در ترکیب با سامانه عامل و یک ایستگاه کاری؛
- یک سامانه عامل در ترکیب با یک ایستگاه کاری؛

• کارت هوشمند مدار مجتمع؛
• رمزنگاری پردازنده مشترک از یک کارت هوشمند مدار مجتمع؛
• شبکه‌های محلی از جمله تمام پایانه‌ها، سرورها، تجهیزات شبکه و نرم افزار؛
• پایگاه داده نرم افزار به استثنای نرم افزار سرویس گیرنده از راه دور که به طور معمول با آن پایگاه داده نرم‌افزار ارتباط برقرار می‌کند.

۵-۲-۱ نمایش‌های متفاوت از TOE

در این استاندارد ملی، TOE می‌تواند در نمایش‌های مختلف از جمله (برای یک نرم افزار TOE) رخ دهد:
• فهرست فایلهای موجود در یک سامانه مدیریت پیکربندی؛
• یک کپی اصلی، که به تازگی ترجمه شده؛
• یک جعبه حاوی یک CD-ROM و کتابچه راهنما، آماده است تا به مشتری تحویل شود؛
• نسخه نصب شده و عملیاتی.
همه این‌ها به عنوان یک TOE در نظر گرفته می‌شود و هر جا که اصطلاح «TOE» در باقی مانده این استاندارد ملی مورد استفاده قرار می‌گیرد، متن معنایی که نمایش داده می‌شود را تعیین می‌کند.

۵-۲-۲ تنظیمات مختلف TOE

به طور کلی، محصولات فناوری اطلاعات را از راههای بسیاری می‌توان پیکربندی کرد: نصب با روش‌های مختلف ، با گزینه‌های مختلف فعال یا غیرفعال شده. همان طور که، در طول ارزیابی این استاندارد ملی، مشخص خواهد شد که آیا TOE منطبق با نیازهای خاص است، این انعطاف پذیری در تنظیمات ممکن است منجر به ایجاد مشکلاتی شود، همچنان که تمام تنظیمات، ممکن است TOE باید الزامات را برآورده کنند. به این دلایل، در اغلب موارد قسمت راهنمای TOE به شدت تنظیمات ممکن برایTOE را محدود می‌کند. که عبارت است از: راهنمایTOE از راهنمای کلی محصولIT ممکن است متفاوت باشد.
یک مثال سامانه عامل آن محصول است. این محصول را می‌تواند به راههای بسیاری پیکربندی شود (به عنوان مثال نوع کاربران، تعداد کاربران، انواع اتصالات خارجی مجاز / غیرمجاز، گزینه‌های فعال / غیرفعال و غیره).
اگر محصول IT همان TOE است ، و در برابر مجموعه ای مناسب از الزامات، ارزیابی شده است، پیکربندی باید خیلی سفت و سخت تر کنترل شود، همان طور که بسیاری از ویژگی‌ها (مانند این که این امکان را می‌دهدکه همه انواع اتصال به شبکه‌های خارجی و یا مدیر سامانه نیاز به تصدیق هویت ندارند) منجر به برآورده کردن الزامات نمی‌شوند
به همین دلیل، به طور معمول تفاوت بین راهنمای محصول IT(اجازه تنظیمات بسیاری را می‌دهد) و راهنمای TOE (اجازه تنها یک تنظیم یا فقط تنظیماتی که مرتبط با امنیت است را می‌دهد) وجود دارد.

یادآوری- اگر راهنمای TOE هنوز هم اجازه بیش از یک پیکربندی را می‌دهد، این تنظیمات جمعی "TOE" نام دارند و هر یک از این پیکربندی‌ها باید الزامات مرتبط با TOE را برآورده کنند.

۵-۳ مخاطب مورد نظر این استاندارد

در ارزیابی ویژگی‌های امنیتی محصولات و سامانه‌های فناوری اطلاعات، سه گروه با سلیقه‌های کلی وجود دارد: مصرف کنندگانTOE، تولید کنندگان TOE و افرادی که TOE را ارزیابی می‌نمایند.معیاری که در این سند ارائه شد، جهت پشتیبانی از نیازهای کلیه این سه گروه سازمان دهی شده است. تمامی آنها، به عنوان کاربران اصلی این استاندارد ملی در نظر گرفته می‌شود. کلیه این گروه‌ها می‌توانند از معیار همانطور که در پاراگراف‌های زیر توضیح داده شده است، استفاده نمایند.

۵-۳-۱مصرف کنندگان

این استاندارد ملی، نقش مهمی را در فنون پشتیبانی جهت انتخاب مصرف‌کننده الزامات امنیتی فناوری اطلاعات برای بیان نمودن نیازهای سازمانی آنها ایفا می‌کند. جهت حصول اطمینان از این امر که ارزیابی، نیازهای مصرف‌کنندگان را به عنوان هدف اصلی و تطابق برای فرآیند ارزیابی برآورده می‌کند ، این استاندارد ملی به صورت مکتوب نوشته می‌شود.

مصرف‌کنندگان می‌توانند از نتایج ارزیابی‌ها جهت کمک در تصمیم‌گیری درباره اینکه سامانه یا محصول، نیازهای امنیتی آنها را برآورده می‌سازد، استفاده نمایند. این نیازهای امنیتی، به طور نمونه به عنوان نتایج تحلیل ریسک و مسیر خط‌مشی شناخته شده است. مصرف‌کنندگان همچنین می‌توانند از ارزیابی جهت مقایسه محصولات یا سامانه‌های مختلف استفاده کنند. معرفی الزامات تضمین از طریق سلسله مراتب، از این نیاز پشتیبانی می‌کند.

این استاندارد ملی به خصوص در گروه‌های مصرف‌کننده و انجمن‌های مورد نظر، ساختاری مستقل تشکیل می‌دهد که پروفایل (PP) را جهت بیان الزامات ضروری آنها برای اقدامات امنیتی فناوری اطلاعات در TOE ، در اختیار مصرف‌کنندگان قرار می‌دهد.

۵-۳-۲ تولید کنندگان

هدف این استاندارد ملی، را می‌توان در پشتیبانی از تولیدکنندگان در آماده‌سازی و کمک در ارزیابی محصولات یا سامانه‌های آنها و در شناسایی الزامات امنیتی که توسط هر یک از محصولات یا سامانه‌های آنها برآورده می‌شود، بیان نمود. این امر نیز کاملا امکان پذیر می‌باشد که روش‌های ارزیابی مشترک که به صورت بالقوه‌ای به همراه توافق شناخت دو طرفه برای نتایج ارزیابی می‌باشد به این استاندارد ملی امکان بیشتری را در جهت پشتیبانی از فردی غیر از تولید کننده TOE در فراهم نمودن و کمک به ارزیابی TOE تولیدکنندگان می‌دهد.

سپس می‌توان از ساختارهای این استاندارد ملی جهت درخواست نمودن این امر که TOEبا الزامات شناخته شده بوسیله عملیات امنیتی خاص و تضمین‌های ارزیابی شده تطابق دارد، استفاده کرد. هر یک از الزامات TOE در ساختارهای مستقل از پیاده سازی، اهداف امنیتی (ST) را تشکیل می‌دهند. یک یا تعداد بیشتری از پروفایل‌های محافظتی، ممکن‌است الزاماتی را از مبنای مصرف‌کننده اصلی فراهم کنند.

این استاندارد ملی، به توضیح عملیات امنیتی که تولید کننده می‌تواند آن را در TOE دربرگیرد، می‌پردازد. این استاندارد ملی را می‌توان جهت تعیین مسئولیت‌ها و اقداماتی جهت پشتیبانی از دلایلی که جهت پشتیبانی از

ارزیابی TOE مورد نیاز می‌باشد، مورد استفاده قرار داد. این امر همچنین محتوا و ارائه مدارک را مشخص می‌نماید.

۵-۳-۳ ارزیاب‌ها

این استاندارد ملی، دارای معیاری می باشد که در زمان قضاوت درباره تطابق TOEها با الزامات امنیتی آنها توسط ارزیاب‌ها به کار گرفته می‌شود. این استاندارد ملی، مجموعه‌ای از اقدامات کلی انجام شده توسط ارزیاب‌ها و عملیات امنیتی جهت اجرای این اقدامات را توضیح می‌دهد. توجه داشته باشید که این استاندارد ملی، رویه‌هایی را جهت انجام این اقدامات مشخص نساخته است.

۵-۳-٤ سایر موارد

در حالی که این استاندارد ملی ، مشخصه‌ها و ارزیابی ویژگی‌های امنیتی فناوری اطلاعات TOEها را برنامه‌ریزی می‌کند، ممکن است همچنین به عنوان موضوع مرجع برای کلیه گروه‌های ذینفع یا مسئولیت برای امنیت فناوری اطلاعات مفید واقع شود.برخی از گروه‌های ذینفع اضافی که می‌توانند از اطلاعات موجود در این استاندارد ملی استفاده نمایند، به شرح زیر می باشند:

الف- مسئولان سامانه و مقامات امنیت سامانه که مسئول تعیین و برآورده‌کردن خط‌مشی‌های امنیتی فناوری اطلاعات و الزامات می باشند؛

ب) مخاطبین داخلی و خارجی که مسئول ارزش‌یابی مناسب بودن امنیت سامانه می‌باشند؛

پ) معماران و طراحان امنیتی که مسئول ویژگی‌های امنیتی ظرفیت سامانه‌های فناوری اطلاعات می باشند؛

ت) افراد مجازی که مسئول پذیرش سامانه فناوری اطلاعات جهت کاربرد آن در محیطی خاص می باشند؛

ث) ضامن‌های ارزیابی که مسئول درخواست و پشتیبانی از ارزیابی می باشند؛

ج) مقامات ارزیابی که مسئول مدیریت و نظارت بر برنامه‌های ارزیابی امنیتی فناوری اطلاعات می باشند.

۵-٤ قسمت‌های مختلف این استاندارد ملی

این استاندارد ملی ، به عنوان مجموعه‌ای از قسمت‌های مجزا اما مربوط به هم همان طور که در زیر توضیح داده شده است، نشان داده می‌شود. اصطلاحات به کار رفته در شرح این قسمت‌ها، در بند ۵ توضیح داده شده است.

الف- **قسمت ۱، مقدمه و نمونه کلی**[1]، مقدمه‌ای برای این استاندارد ملی می‌باشد. این قسمت، مفاهیم و دستورالعمل‌های کلی ارزیابی امنیت فناوری اطلاعات را مشخص نموده و نمونه‌ای کلی از ارزیابی را نشان می‌دهد. قسمت ۱ همچنین ساختارهایی را برای اهداف امنیتی فناوری اطلاعات جهت انتخاب و تعیین الزامات امنیتی فناوری اطلاعات و ثبت مشخصه‌های سطح بالا برای محصولات و سامانه، معرفی می‌کند. علاوه بر این، کاربرد هر قسمت از این استاندارد ملی بر حسب هر یک از مخاطبین مورد نظر، توضیح داده شده است.

1- Introduction and general model

ب) **قسمت ۲، الزامات عملیاتی امنیت**[1]، مجموعه ای از مؤلفه‌های عملیاتی را به عنوان روشی استاندارد جهت بیان نمودن الزامات تضمین برای TOEها ایجاد می‌نماید. قسمت ۲ مجموعه مؤلفه‌ها، خانواده‌ها و سطوح عملیاتی را فهرست می‌کند.

ج) **قسمت۳، الزامات تضمین امنیت**[2]، مجموعه ای از مؤلفه‌های تضمین را به عنوان روشی استاندارد جهت بیان نمودن الزامات تضمین برای TOEها ایجاد می‌نماید. قسمت ۳ مجموعه مؤلفه‌ها، خانواده‌ها و سطوح تضمین را فهرست می‌کند. قسمت ۳ همچنین معیار ارزیابی برای پروفایل‌های محافظتی و STها را تعیین نموده و سطوح تضمین ارزیابی که معیار این استاندارد ملی را جهت درجه بندی تضمین برای TOEها که سطوح تضمین ارزیابی (EALها) نامیده می‌شود، تعیین می‌کند. در پشتیبانی از سه قسمت این استاندارد ملی که در بالا توضیح داده شد، انتظار می‌رود که سایر انواع مستندات نیز منتشر شود که از آن جمله می توان به موضوع منطقی فنی و مستندات راهنما اشاره نمود.

جدول زیر، نحوه استفاده از این استاندارد ملی را جهت دسته بندی سه مخاطب مورد نظر، نشان می دهد.

جدول ۱- طرحی در خصوص « معیار ارزیابی برای امنیت فناوری اطلاعات»

	مصرف کنندگان	تولید کنندگان	ارزیاب‌ها
قسمت۱	به عنوان اطلاعات پیش زمینه و اهدافی که مرجع باشند، مورد استفاده قرار می گیرد. ساختار راهنما برای پروفایل‌های محافظتی.	به عنوان اطلاعات پیش زمینه و مرجعی برای ایجاد الزامات‌وتنظیم‌نمودن مشخصه‌های‌امنیتی برای TOEها،مورداستفاده قرارمی‌گیرد.	به عنوان اطلاعات پیش زمینه و اهدافی که مرجع باشند، مورد استفاده قرار می‌گیرد. ساختارراهنمابرای PPها و STها.
قسمت۲	به عنوان راهنما و مرجع در هنگام تنظیم بیانیه الزامات برای عملیات امنیتی به کار گرفته می‌شود.	به عنوان مرجع در هنگام ارائه بیانیه‌های الزامات عملیاتی‌وتنظیم‌مشخصه‌های عملیاتی برای TOEها به‌کارگرفته می‌شود.	به‌عنوان‌بیانیه‌ای‌الزامی ازمعیارارزیابی‌درهنگام تصمیم‌گیری‌درمورد برآورده‌نمودن‌عملیات امنیتی‌موردنظربه‌طور کارآمد،به‌کارگرفته‌می‌شود.

1- Security functional requirements

2 -Security assurance requirements

قسمت۳	به عنوان راهنما در هنگام تعیین سطوح مورد نیاز جهت تضمین مورد استفاده قرار می گیرد.	به عنوان مرجع در هنگام تفسیر بیانیه‌های الزامات تضمین و تصمیم‌گیری در خصوص روش‌های تضمین TOEها مورد استفاده قرار می‌گیرد.	به عنوان بیانیه‌ای الزامی درمورد معیار ارزیابی در هنگام تعیین تضمین TOEها و در هنگام ارزیابی PPها و PTها مورد استفاده قرار می‌گیرد.

۵-۵- مفهوم ارزیابی

جهت دستیابی به مقایسه جامع‌تری میان نتایج ارزیابی، ارزیاب‌ها باید در چهارچوب کاری، الگوی ارزیابی معتبری که استانداردها را فراهم نموده، کیفیت ارزیابی‌ها را بررسی نموده و قانونی که تسهیلات ارزیابی و ارزیاب‌ها باید از آن پیروی نمایند، را اجرا می‌نماید.

این استاندارد ملی الزاماتی را برای چهارچوب کاری قانونی، عنوان ننموده است. این درحالی‌است که هماهنگی میان چهارچوب‌های قانونی مقامات ارزیابی مختلف جهت دستیابی به هدف شناسایی دو جانبه نتایج چنین ارزیابی‌هایی، ضروری می‌باشد. شکل شماره یک، به معرفی مؤلفه‌های اصلی که موضوع ارزیابی‌ها را تشکیل می دهند، می‌پردازد.

بکارگیری روش‌های ارزیابی مشترک منجر به تکرارپذیری و عینی بودن نتایج می‌شود اما در جای خود کافی نمی‌باشد. بسیاری از معیارهای ارزیابی نیازمند بررسی‌های افراد متخصص و دانش پیش‌زمینه جهت اطلاع از سختی دسترسی به سازگاری می‌باشد. جهت ایجاد هماهنگی در میان یافته‌های حاصل از ارزیابی، نتایج ارزیابی نهایی را می‌توان در فرآیند تائید، وارد نمود. فرآیند تائید، نظارت مستقل نتایج ارزیابی می‌باشد که به تائید یا تصدیق نهایی منجر می‌شود. گواهی تائید، معمولا به طور عموم در دسترس می‌باشد. باید توجه داشته باشیم که فرآیند تائید، روشی جهت حصول هماهنگی بیشتر در برنامه کاربردی معیار امنیتی فناوری اطلاعات می‌باشد.

الگوی ارزیابی، روش و فرآیندهای تائید از مسئولیت‌های مقامات ارزیابی می‌باشد که الگوهای ارزیابی را به اجرا درآورده و خارج از حوزه این استاندارد ملی می‌باشد.

٦ مدل عمومی

٦-١ معرفی مدل عمومی

این قسمت به ارائه مفاهیم عمومی می‌پردازد که در استاندارد (ISO/IEC 15408) ISO/IEC 15408 استفاده شده است، که شامل مضامین مفهومی به کاررفته شده در این استاندارد و همچنین رویکرد ISO/IEC 15408 (ISO/IEC 15408) در بکارگیری از این مفاهیم می‌شود. قسمت دوم و سوم ISO/IEC 15408 که برای کاربران قسمت اول این استاندارد مستندی الزامی در نظر گرفته شده است، در حقیقت بسط مفاهیم و انگاره‌هایی است که رهیافت‌های توضیح داده شده در آن دو قسمت از آنها استفاده می‌کنند. ضمنا مستند CEM برای کاربران ISO/IEC 15408 که علاقه مند به انجام امور ارزیابی هستند قابل استفاده است. هرچند این

قسمت برخی مفاهیم علمی از امنیت فناوری اطلاعات را شامل می‌شود ولی بعنوان یک مستند آموزشی در این قسمت توصیه نمی شود.
استاندارد ISO/IEC 15408 در حوزه امنیت با استفاده از مجموعه ای از مفاهیم و لغات بحث می‌کند. قطعا آشنایی با این مفاهیم و لغات در استفاده از این استاندارد بسیار مفید خواهد بود. هرچند که همه این مفاهیم بسیار کلی بیان شده و محدود به هیچ گروه از مسائل امنیت فناوری اطلاعات که ISO/IEC 15408 در آنها قابل کاربرد است، نمی باشد.

۲-٦ سرمایه‌ها و اقدامات حفاظتی

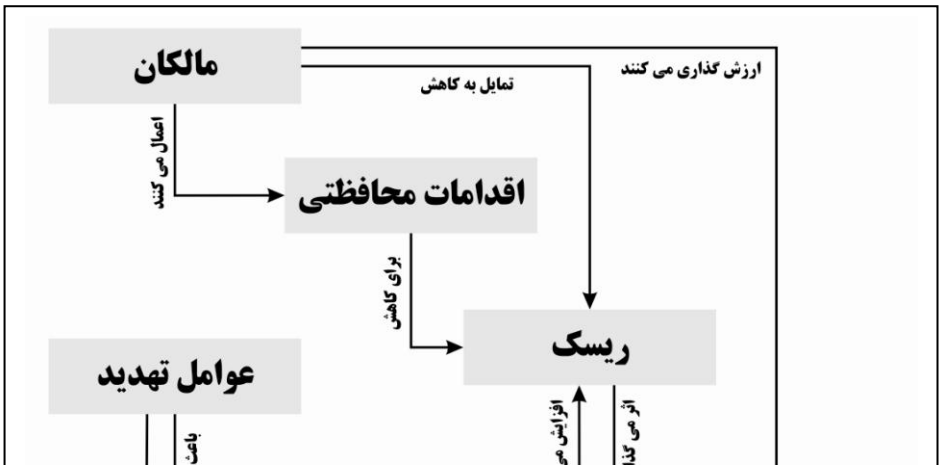
امنیت متوجه حفاظت از سرمایه‌هاست و سرمایه‌ها هستارهایی هستند که بتوان برآن‌ها ارزش گذاری نمود. در ذیل نمونه‌هایی از سرمایه‌ها ذکر شده اند:

- محتوای اطلاعاتی درون یک فایل یا یک سرور
- صحت رأی اخذ شده در انتخابات
- قابلیت دسترس پذیری در یک فرایند تجاری در قالب فضای الکترونیکی
- قابلیت استفاده از یک چاپگر گران قیمت
- دسترسی به تسهیلات طبقه بندی شده

با توجه به اینکه ارزش گذاری بشدت وابسته به موضوع است، تقریبا هرچیزی می‌تواند یک سرمایه تلقی گردد.
محیطی(هایی) که در برگیرنده این سرمایه‌ها است بعنوان محیط عملیاتی نامیده می‌شود. در ذیل مثالهایی (جنبه‌هایی) از محیط‌های عملیاتی داده شده است:

- اتاق رایانه یک بانک
- یک رایانه (از یک) شبکه که به اینترنت متصل است
- یک شبکه محلی LAN
- یک محیط اداری عمومی

بسیاری از سرمایه‌ها به شکل اطلاعاتی هستند که برای برآوردن نیازمندی‌های مالکان آنها در قالب اطلاعات ذخیرشده، پردازش شده و انتقال داده شده توسط محصولات فنآوری اطلاعات قرار می‌گیرند. مالکان اطلاعات به همان قسمت از اطلاعات با هر اندازه ای از کنترل که در اختیار دارند نیازمند دسترسی، توزیع و یا تغییر اطلاعات هستند، از طریق اینگونه اقدامات حفاظتی است که اطلاعات از انواع تهدیدها محافظت می‌شوند. شکل ۲ نشان گر مفاهیم ذکر شده و ارتباط بین آنها می‌باشد.



شکل ۲ – مفاهیم امنیتی و ارتباط بین آنها

شکل ۲ – مفاهیم امنیتی و ارتباط بین آنها

تعیین مرزهای حفاظتی سرمایه‌ها بر عهده مالکانی است که برآن ارزش گذاری می‌نمایند. عوامل واقعی یا مفروض تهدید هم می‌توانند بر ارزش گذاری سرمایه‌ها موثر و به دنبال سوء استفاده از سرمایه‌ها از طریق انجام رفتاری مخالف خواسته مالکان باشند. مثال‌هایی از عوامل تهدید مواردی چون، هکرها، کاربران خطاکار، کاربران غیر خطاکار (خطاهای غیر عمدی)، فرایندهای رایانه و حوادث هستند.

مالکان سرمایه باید تهدیدها را بعنوان عامل‌های بالقوه ای در نظر بگیرند که ارزش سرمایه‌های آنها را کاهش می‌دهد. برخی عوامل محدود کننده امنیتی شامل مواردی چون، کاهش محرمانگی سرمایه، کاهش صحت و کاهش دسترس پذیری سرمایه می‌باشد ولی فقط به این موارد محدود نمی شود.

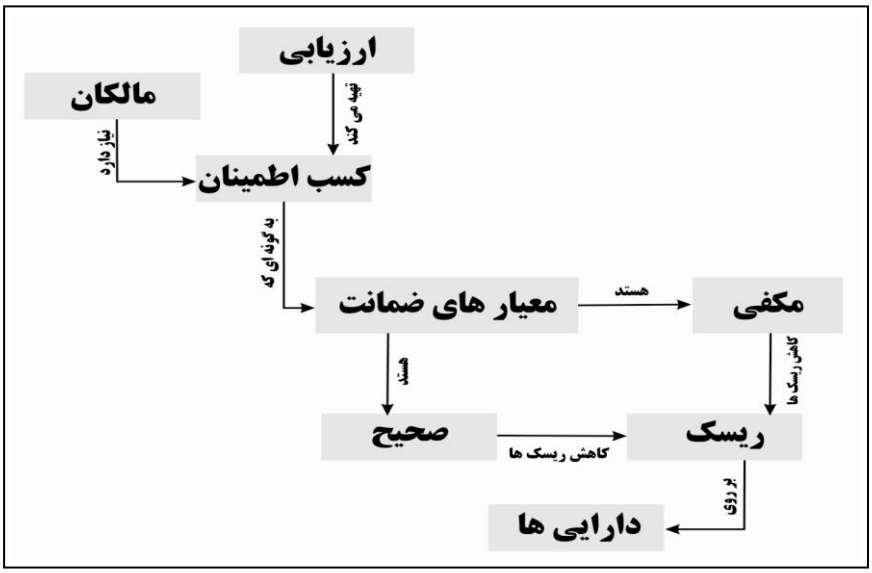
تهدیدها میزان ریسک بر سرمایه‌ها را هم افزایش می‌دهند، بر مبنای هر تحلیل و احتمالی که تهدیدها تشخیص داده شدند باید اثر آن‌ها بر سرمایه‌های اطلاعاتی نیز مشخص شوند. بدین ترتیب اقدامات حفاظتی می‌تواند منجر به کاهش ریسک بر سرمایه شود. اقدامات حفاظتی می‌تواند شامل اقداماتی مبتنی بر فناوری (همانند دیواره‌های آتش و کارت‌های هوشمند) و یا غیر وابسته به فنآوری (مانند حفاظت فیزیکی و زیرروالها)باشد. برای مطالعه در انواع اقدامات حفاظتی امنیتی (کنترلهای امنیتی) می‌توانISO/IEC 27002 , SO/IEC 27001 را مبنای مطالعه قرار داد.

مالکان سرمایه‌ها ممکن است مسئولیت این دارایی‌ها را هم برعهده داشته باشند، بنابراین باید قادر به تصمیم سازی در خصوص پذیرش ریسک‌های حاصل از تهدیدها بر سرمایه‌ها باشند.

دو عنصر مهم در دفاع از این تصمیم سازی به شرح ذیل بیان شده است:

- اقدامات حفاظتی کافی است: اگر اقدامات، کارکردی معادل با آنچه ادعا شده است، داشته باشند، با تهدیدهای وارد بر سرمایه‌ها مقابله شده است.
- اقدامات حفاظتی درست هستند: اقدامات هرآنچه ادعا شده است به درستی انجام دهند (انتخاب‌های درست نتایج مورد انتظار را بدهد).

بسیاری از مالکان اطلاعات با نبود دانش، تجربه و منابع مورد نیاز برای قضاوت بر صحت اقدامات حفاظتی مواجه هستند و از طرفی هم قصد اعتماد بر اظهارات توسعه دهندگان این گونه اقدامات هم ندارند. این مصرف کنندگان می‌توانند برای کسب و یا افزایش اطمینان بر کافی بودن و یا صحت همه یا قسمتی از اقدامات حفاظتی مورد نظر خود این اقدامات را مورد ارزیابی قرار دهند.



شکل ۳ – مفاهیم ارزیابی و ارتباط بین آنها

٦-٢-١ بسندگی اقدامات حفاظتی

در یک ارزیابی، بسندگی اقدامات حفاظتی از طریق تحلیل ساختاری با عنوان هدف امنیت ارزیابی تحلیل می‌شود. در ادامه مروری ساده بر این ساختار ارائه می‌شودف برای اطلاع از جزئیات بیشتر و تکمیلی پیوست الف مطالعه شود.

مستند هدف امنیتی با توصیف دارایی و تهدیدهایی که بر دارایی قرار دارند آغاز می‌شود. در ادامه این مستند اقدامات حفاظتی (به در قالب قسمت اهداف امنیتی) توضیح داده می‌شود و بسندگی اقدامات حفاظتی برای کنترل تهدیدها نشان داده می‌شود که این خود منوط به این است که اقدامات تعیین شده رفتار منطبق با ادعای بیان شده داشته باشند.

مستند هدف امنیتی این گونه اقدامات را به دو گروه تقسیم می‌کند:

الف- اهداف امنیتی برای هدف (محصول) مورد ارزیابی (TOE): این قسمت به بیان مجموعه اقداماتی می‌پردازد که در تصمیم گیری‌ها در روند ارزیابی منجر به صحت و درستی کنترل تهدیدها می‌شوند.

ب) اهداف امنیتی برای محیط عملیاتی: این قسمت به بیان مجموعه اقداماتی می‌پردازد که در تصمیم گیری‌ها در روند ارزیابی منجر به صحت و درستی کنترل تهدیدها نمی شوند.

دلایل تقسیم بندی ذکر شده بالا:

- استاندارد ISO/IEC 15408 فقط برای ارزیابی صحت اقدامات حفاظتی وابسته به فنآوری طراحی شده است. بنابراین کلیه اقدامات غیر وابسته به فنآوری اطلاعات (برای مثال، حفاظت فیزیکی و انسانی، روالهای سازمانی) همواره در محدوده محیط عملیاتی قرار می‌گیرند.
- ارزیابی صحت و درستی اقدامات حفاظتی هزینه زمانی و مالی در پی دارد و مسلما اعمال این ارزیابی‌ها برای همه انواع اقدامات وابسته به فنآوری غیر ممکن می‌نماید.
- صحت برخی از اقدامات حفاظتی وابسته به فنآوری می‌تواند از طریق ارزیابی‌های دیگری تعیین شود که این مسئله نشان می‌دهد انجام دوباره کاری مقرون به صرفه اقتصادی و بهره ور نخواهد بود.

برای (محصول) هدف امنیتی (اقدامات حفاظتی صحیح در طول ارزیابی سنجیده می‌شوند)، مستند هدف امنیتی نیازمند جزئیات بیشتری از اهداف امنیتی در مورد نیازمندی‌های کارکردی امنیت محصول (Security Functional Requirements - SFRs) می‌باشد. این نوع نیازمندی‌ها تحت یک قالب و زبان استاندارد در قسمت دوم استاندارد ISO/IEC 15408 بیان شده اند تا اطمینان از سهولت مقایسه و دقت کافی را ایجاد کند.

به طور خلاصه، مستند هدف امنیتی موارد ذیل را نشان می‌دهد:

- مجموعه نیازمندی‌های غیر کارکردی که همه اهداف امنیتی محصول را پوشش دهد.
- اهداف امنیتی محصول و اهداف امنیتی محیط عملیاتی پیرامون آن که مجموعا برای کنترل تهدیدها الزامی هستند.
- مجموع نیازمندی‌های غیر کارکردی امنیت محصول و اهداف امنیتی محیط عملیاتی پیرامون آن باید همه تهدیدها را پوشش دهند و کنترل کنند.

بعنوان نتیجه باید گفت، یک محصول درست یعنی محصولی که همه نیازمندی‌های غیر کارکردی خود را پوشش داده باشد، در ادغام با محیط عملیاتی مناسب و درست یعنی محیطی که اهداف امنیتی انتخاب شده را رعایت کرده باشد، با هم می‌توانند تهدیدها را پوشش دهند. در دو قسمت بعدی به طور مجزا به هر کدام از این دو مبحث به تفصیل می‌پردازیم.

۲-۲-۶ صحت محصول

یک محصول ممکن است که به شکل نادرست طراحی و پیاده سازی شده باشد و در نتیجه شامل مجموعه ای از خطاها باشد که نهایتا منجر به ظهور حفره‌های امنیتی در آن شود. با سوء استفاده از این حفره‌ها، مهاجمین به راحتی می‌توانند منجر به خرابی و/یا سوء استفاده از سرمایه‌ها شوند.

حفره‌های امنیتی ممکن است از طریق برخی خطاهای تصادفی و ناخواسته در طول فرایند توسعه، طراحی (معماری)های ضعیف، افزودن کدهای مخرب به صورت عمدی و اجرای تست‌های ضعیف ایجاد شوند.

برای تعیین صحت یک محصول، اقدامات بسیار متنوعی می‌توان انجام داد مانند:

- تست محصول (TOE)
- سنجش انواع جنبه‌های طراحی محصول
- سنجش امنیت فیزیکی محیط توسعه محصول

مستند هدف امنیتی تحت یک قالب ساختار یافته همه این گونه فعالیت‌ها را به شکل مدون وبا نام نیازمندی‌های ارزیابی امنیت (SARs[1]) بیان می‌کند. این نوع نیازمندی‌ها تحت یک قالب و زبان استاندارد در قسمت سوم استاندارد ISO/IEC 15408 بیان شده اند تا اطمینان از سهولت مقایسه و دقت کافی را ایجاد کند.

اگر نیازمندی‌های ضمانت امنیت پوشش داده شود، بدین معنا است که محصول تولید شده به شکل ضمانت شده ای در مقابل حفره‌های موجود و تهدیدها آتی از خطر سوء استفاده توسط مهاجمین در امان است. میزان ضمانت از صحت محصول تولید شده وابسته به مجموعه نیازمندی‌های ضمانتی است که در ابتدا تعیین می‌شود. یک مجموعه نیازمندی‌های ضمانتی ضعیف منجر به میزان کمی از ضمانت امنیت می‌شود و در مقابل مجموعه قوی ضمانت بیشتری را ارائه می‌کند.

۶-۲-۳ صحت محیط عملیاتی

محیط عملیاتی نیز ممکن است دچار طراحی نامناسب و یا پیاده سازی غیر صحیح شود که ممکن است خطاهایی موجود در محیط حفره‌های امنیتی را ایجاد کند. با آشکار شدن این حفره‌ها، هنوز ممکن است مهاجمین موجب خربی و/یا سوء استفاده از سرمایه‌ها شوند.

هر چند استاندارد ISO/IEC 15408 به طور مستقیم تضمینی برای ایجاد محیط عملیاتی مناسب ندارد و بعبارت دیگر ارزیابی امنیت محیط عملیاتی موضوع بحث ISO/IEC 15408 نیست (بند بعدی را مطالعه کنید).

تا آنجایی که به ارزیابی مربوط می‌شود، صحت محیط عملیاتی در مرحله تعیین اهداف امنیتی برای محیط پیرامون به طور کامل باید دیده شود.

این مسئله منعی برای مصرف کنندگان به جهت اتخاذ تصمیم در خصوص محیط پیرامون خود نیست، روشهایی مانند آنچه در ذیل ذکر شده در این حیطه مناسب است:

اگر یک سامانه عامل بعنوان محصول مورد ارزیابی است، اهداف امنیتی محیط پیرامون این گونه بیان می‌شود که"محیط عملیاتی باید این اطمینان را ایجاد کند که هر هستار در شبکه نا مطمئن (برای مثال اینترنت) فقط از طریق پروتکل FTP به محصول (در اینجا سامانه عامل) دسترسی دارد"، مصرف کننده می‌تواند با انتخاب یک دیواره آتش و پیکربندی مناسب آن برای دسترسی امن به پروتکل FTP از هدف امنیتی خود (محصول، در اینجا سامانه عامل) محافظت کند.

اگر اهداف امنیتی برای محیط عملیاتی اینگونه بیان شد که«محیط عملیاتی باید این اطمینان را ایجاد که همه پرسنل اداری[2] رفتار عاندانه نداشته باشند»،مصرف کننده می‌تواند در قرار دادهای خود با پرسنل موارد قانونی رفتارهای کارشکنانه را بیان کند، اما این تصمیم گیری‌ها قسمتی از ارزیابی ISO/IEC 15408 نیست.

۶-۳ ارزیابی

استاندارد ISO/IEC 15408 دو نوع ارزیابی را پیشنهاد می‌کند، ارزیابی(مستند هدف امنیتی /محصول مورد ارزیابی) ST/TOE که در ذیل توضیح داده می‌شود و ارزیابی (رخ‌نمون محافظتی) PP که در قسمت سوم این

1- Security Assurance Requirements

2- Administrative Personnel

استاندارد ملی توضیح داده شده است. در بسیاری از مواردی، ISO/IEC 15408 از لغت ارزیابی (بدون هیچ کلمه توصیفی دیگری) برای ارجاع دادن به ارزیابی ST/TOE استفاده می‌کند.

در استاندارد ISO/IEC 15408 فرایند ارزیابی ST/TOE در دو مرحله انجام می‌شود:

الف- ارزیابی ST، به گونه ای که تعیین شود آیا به قدر کافی و درست محصول و محیط پیرامون آن تعریف شده باشند.

ب) ارزیابی محصول، به گونه ای که صحت محصول تعیین شود. همانطور که قبلا گفته شد، ارزیابی محصول مرتبط با ارزیابی محیط پیرامون آن نیست.

ارزیابی ST از طریق ضوابط ارزیابی مستند هدف امنیتی انجام می‌شود (در قسمت سوم این استاندارد تعریف شده است). روشی برای پیاده سازی ضوابط تعیین شده در کلاس ASE، در متدولوژی ارزیابی بطور خلاصه باید تعیین شده باشد.

ارزیابی محصول بسیار پیچیده تر است. ورودی‌های مهم فرایند ارزیابی محصول عبارتند از: مدراک و مستندات قابل ارزیابی که شامل خود محصول و مستند هدف امنیتی است و این ادله در محیط توسعه تهیه می‌شوند، مانند مستندات طراحی و نتایج تست توسعه دهنده.

ارزیابی محصول اصرار بر استقرار نیازمندی‌ها و ضوابط تضمین امنیت (SARs) (برگرفته شده از مستند هدف امنیتی) بر مدارک ارزیابی است. متد مورد استفاده برای ارزیابی باید وجود هر نیازمندی ضمانت امنیت را تعیین کند.

چگونگی مستند سازی نتایج بکارگیری نیازمندی‌های ضمانت امنیت، نوع گزارشات مورد نیاز و جزئیات آن در هر دو متد ارزیابی تحت شمای ارزیابی انجام شده تعیین می‌شود.

نتایج ارزیابی محصول شامل:

- همه نیازمندی‌های ضمانت که بیانگر سطح مشخص از ضمانت امنیت محصول است، مطابق آنچه که در مستند هدف امنیتی بیان شده و باید محصول نیازمندی‌های کارکردی اظهار شده را برآورده سازد، پوشش داده نشده است.
- همه نیازمندی‌های ضمانت که بیانگر سطح مشخص از ضمانت امنیت محصول است، مطابق آنچه که در مستند هدف امنیتی بیان شده و باید محصول نیازمندی‌های کارکردی اظهار شده را برآورده سازد، پوشش داده شده است.

ارزیابی محصول ممکن است پس از انجام فرایند توسعه و در زمان اتمام آن اجرا شود و یا اینکه به صورت موازی در زمان توسعه محصول انجام شود.

روش بیان نتایج ارزیابی ST/TOE در بند ۱۰ توضیح داده شده است. این نتایج همچنین موجب شناسایی رخ‌نمون محافظتی و بسته‌ها[1] به گونه که مطابق با ادعای محصول باشد، می‌شود، این ساختار در قسمت بعدی توضیح داده شده است.

1- Packages

۷ مناسب سازی نیازمندی‌های امنیتی

۷-۱ عملیات

مولفه‌های کارکردی و ضمانتی ISO/IEC 15408، ممکن است به همانگونه که در قسمت دوم و سوم این استاندارد ذکر شده است مورد استفاده قرار گیرد، یا طی عملیات مجازی سازگاری و مناسب سازی ایجاد شود. زمانی که از عملیات استفاده می‌کنید، نویسنده ST/PP (رخنمون محافظتی/ هدف امنیتی) باید مراقب وابستگی‌ها بین نیازمندی‌ها به گونه ای که مشخص شده است باشد. عملیات مجاز از مجموعه عملیات تعریف شده زیر انتخاب می‌شود:

- تکرار: از یک مولفه بیش از یک بار تحت انواع عملیات مختلف اجازه استفاده وجود دارد.
- تخصیص: پارامترهای مشخص مجاز به تخصیص می‌باشد.
- انتخاب: انتخاب یک یا چند موضوع معین از یک مجموعه مشخص مجاز می‌باشد.
- پایش: اضافه کردن یا کاهش برخی جزئیات مجاز می‌باشد.

تخصیص و انتخاب فقط بر مولفه‌هایی که مشخص شده که مجازمی باشد، قابل اجراست. عملیات تکرار و پایش برای همه مولفه‌ها مجاز است. جزئیات بیشتر عملیات در قسمت ذیل به تفصیل ارائه شده است.

پیوست قسمت دوم استاندارد ISO/IEC 15408 راهنمایی لازم برای اجرای کامل و معتبر عملیات انتخاب و تخصیص ارائه کرده است. این راهنما قواعد و اصول چگونگی تکمیل شدن عملیات را تهیه می‌کند، و این قواعد باید رعایت شوند مگر آنکه نویسنده ST/PP عنوان کرده باشد:

الف-« None»، برای تکمیل عملیات انتخاب اگر و فقط اگر به وضوح بیان شده باشد مورد استفاده قرار می‌گیرد. فهرست تهیه شده برای تکمیل انتخاب‌ها باید غیر تهی باشد، اگر گزینه None، انتخاب شود، هیچ عمل انتخاب اضافه تری نمی تواند انتخاب شود. اگر None بعنوان یک گزینه در عمل انتخاب عنوان نشده باشد، می‌توان مجموعه ای از عملیات انتخاب را با عملگر AND و OR ادغام و استفاده نمود مگر اینکه بطور واضح بیان شود فقط یک عمل انتخاب صورت گیرد.

عملیات انتخاب ممکن است در صورت نیاز با عملیات تکرار ادغام شود. در این موارد، قابلیت اجرایی گزینه انتخاب شده از عمل انتخاب نمی بایست با موضوعات دیگر عملیات‌های تکرار هم پوشانی داشته باشد، نظر باینکه این عملیات از نظر مفهوم منحصر به فرد هستند.

ب) برای تکمیل عمل تخصیص، همانگونه که در پیوست قسمت دوم استاندارد ISO/IEC 15408 بیان شده است، باید برای تصمیم سازی در زمانی که None برای تکمیل عملیات معتبر است، بررسی شود.

۷-۱-۱ عملیات تکرار

این عملیات بر همه مولفه‌ها قابل اجرا است. نویسنده PP/ST با استناد به این قابلیت مجموعه ای از نیازمندی‌ها را بر مبنای یک مولفه معین در ISO/IEC 15408 بیان می‌کند. هر تکرار مولفه باید از دیگر تکرارهای همان مولفه متفاوت باشد، همانطوری که تکمیل تخصیص و انتخاب و به‌کارگیری پایش با روشهای دیگر این گونه است.

هر عمل تکرار باید بصورت منحصر بفرد شناسایی شود تا بصورت شفاف و مستدل هر نیازمندی قابل رهگیری باشد.

نکته بسیار مهم در مورد عملیات تکرار این است که امکان اجرای عمل تخصیص بر محدوده ای از فهرست مقادیر به جای عمل تکرار مجاز است. در این مورد نویسنده ST/PP مناسب ترین روش را باید ذکر کند، البته باید نویسنده در نظر داشته باشد که ادله مرتبط با برآورده شدن نیازمندی توسط این مجموعه مقادیر بصورت جداگانه و یا گروه مقادیر مدون گردد. نویسنده باید رهگیری هر نیازمندی بصورت منحصر بفرد را در هر حالت در نظر داشته باشد.

۷-۱-۲ عملیات تخصیص

عملیات تخصیص زمانی اتفاق می‌افتد که مولفه ای با مجموعه ای از پارامترها بیان شود و مقدار گذاری این پارامترها توسط نویسنده ST/PP انجام می‌شود. پارامترها می‌تواند مجموعه نامحدودی از متغیرها باشد، یا توسط قاعده ای محدود به محدوده مشخصی از مقادیر می‌باشد.

هرجا که عنصری در رخ‌نمون محافظتی شامل عمل تخصیص باشد، نویسنده PP باید یکی از چهار عمل زیر را انجام دهد:

الف- رها کردن عمل تخصیص به شکل غیر کامل. برای مثال نویسنده PP مولفه FIA_AFL.1.2 را عینا همانگونه که در استاندارد بیان شده ذکر کند، یعنی: "هرگاه تعداد مشخص شده ای از تلاش‌های ناموفق از احراز هویت اتفاق بیافتد، TSF باید {تخصیص: فهرستی از عملیات}"

ب- تخصیص کامل. برای مثال نویسنده PP مولفه FIA_AFL.1.2 را بدین گونه بنویسد: " هرگاه تعداد مشخص شده ای از تلاش‌های ناموفق از احراز هویت اتفاق بیافتد، TSF باید از هرگونه انقیاد درهر شکل هستار خارجی تلاش کننده در آینده جلوگیری کند."

پ- تخصیص محدود. برای گسترش محدودیت بر محدوده مقادیر مجاز. برای مثال نویسنده PP مولفه FIA_AFL.1.1 را بدین گونه بنویسد:«TSF باید تشخیص دهد هرگاه {تخصیص:یک عدد مثبت صحیح بین ۴ تا ۹} تلاش ناموفق در احراز هویت اتفاق افتاد .....».

ت) انتقال تخصیص به یک انتخاب وبه موجب آن محدود کردن تخصیص. برای مثال نویسنده PP مولفه FIA_AFL.1.2 را بدین گونه بنویسد: « هرگاه تعداد مشخص شده ای از تلاش‌های ناموفق از احراز هویت اتفاق بیافتد، TSF باید {انتخاب: از انقیاد کاربر به هر شکل جلوگیری کند، به مدیر اطلاع دهد}».

هرجا که عنصری در یک مستند هدف امنیتی شامل عملیات تخصیص باشد، نویسنده ST باید تخصیص کامل همانطور که در بند (ب) تعریف شده است را استفاده کند. به هیچ عنوان موارد الف، پ و ت برای مستند هدف امنیتی مجاز نیستند.

مقادیر انتخاب شده در موارد ب،ج و د باید با نوع نیازمندی تخصیص سازگار باشد.

هرگاه عمل تخصیص توسط یک مجموعه تکمیل شود (برای مثال موضوعات)، باید مجموعه ای از موضوعات فهرست شود، اما برخی از توصیف‌های مجموعه از عناصر آن می‌تواند همانند زیر دسته بندی شود:

- همه موضوعات

- همه موضوعات از نوع خاص
- همه موضوعات بجزء یک موضوع خاص
- مادامی که موضوعات تعریف شده، مشخص هستند

۷-۱-۳ عملیات انتخاب

عملیات انتخاب زمانی اتفاق می‌افتد که مولفه ای داده شده شامل عنصری است که نویسنده PP/ST چندین انتخاب را برای اجرای آن ایجاد کرده است.

هرجا که یک عنصر از PP شامل عمل انتخاب باشد، نویسنده PP ممکن است یکی از سه عمل زیر را انجام دهد:

الف- رها کردن عمل انتخاب به صورت غیر کامل

ب- طراحی عمل انتخاب با ایجاد یک یا چند راه حل برای گزینش

پ)ارائه انتخاب محدود با امکان گذر از برخی گزینه‌ها، ولی دو گزینه یا بیشتر را برای انتخاب باید قرار دهد.

زمانی که یک عنصر در مستند هدف امنیتی شامل عمل انتخاب است، نویسنده باید عملیات انتخاب را به صورت کامل پیاده سازی کند، همانطوری که در قسمت (ب) گفته شده است. گزینه الف و ج در طراحی مستند هدف امنیتی مجاز نیستند.

گزینه یا گزینه‌هایی که توسط حالت ب و پ انتخاب شده اند، باید توسط گزینه‌های تهیه شده توسط عمل انتخاب اجرا شوند.

۷-۱-٤ عملیات پایش

عملیات پایش بر هر نیازمندی قابل اجرا است. نویسنده PP/ST از طریق تغییر نیازمندی عمل پایش را انجام می‌دهد. اولین وظیفه در عملیات پایش این است که محصول (TOE) نیازمندی‌های پایش شده را پوشش دهد و همچنین نیازمندی‌های پایش نیافته را نیز در محتوای PP/ST برآورده سازد. (برای مثال نیازمندی‌های پایش شده باید بسیار سخت گیرانه تر از نیازمندی‌های اصلی باشد.) اگر عملیات پایش این وظیفه را انجام ندهد، نتایج پایش نیازمندی اینگونه بنظر می‌رسد که نوعا نیازمندی‌های اضافی و سربارگونه هستند.

تنها استثناء در این وظیفه این است که نویسنده PP/ST مجاز به پایش مستند نیازمندی‌های کارکردی SFR برای به کار بستن بر قسمتی از موضوعات، اهداف، عملیات و خصیصه‌های امنیتی و/یا هستارهای خارجی است و البته نه بر همه آنها.

هرچند، این استثناء بدین معنا نیست که مستند نیازهای کارکردی امنیت، که خود برگرفته از یک PP مستدل و مورد تایید است را بتوان پایش کرد و برای قسمت کوچکتری از موضوعات، اهداف، عملیات، خصیصه‌های امنیتی و/یا هستارهای خارجی به کار بست.

وظیفه دوم برای عملیات پایش این است که باید به مولفه‌های اصلی مرتبط باشد.

یک حالت خاص از عملیات پایش، یک عمل پایش سفارشی است، به گونه ای که تغییر کوچکی در نیازمندی‌ها ایجاد می‌شود، برای مثال: بازنویسی جملات به دلیل سازگاری با قواعد زبان انگلیسی، یا ایجاد قابلیت فهم بیشتر برای خوانندگان. این حالت تغییر در معنای نیازمندی را به هیچ شکل مجاز نمی دارد.

۷-۲طرز وابستگی بین مولفه‌ها

وابستگی ممکن است بین مولفه‌ها موجود باشد. وابستگی زمانی نمود پیدا می‌کند که یک مولفه به تنهایی کافی نبوده و برای برآورده ساختن نیازکارکردی امنیت یا نیاز ضمانتی امنیت باید با یک مولفه دیگر در نظر گرفته شود.

مولفه‌های کارکردی در قسمت دوم استاندارد ISO/IEC 15408 بطور معمول بر دیگر مولفه‌های کارکردی وابستگی دارند و به همین ترتیب برخی مولفه‌های ضمانتی در قسمت سوم این وابستگی را دارند. وابستگی‌های بین مولفه ای قسمت دوم بر روی مولفه‌های قسمت سوم استاندارد ISO/IEC 15408 قابل تعریف است. هرچند مانعی برای وابستگی بین مولفه‌های کارکردی امنیت توسعه داده شده با مولفه‌های ضمانت وجود ندارد و برعکس.

وابستگی بین مولفه‌ها بر اساس تعریف‌های بیان شده در قسمت دوم و سوم استاندارد ISO/IEC 15408 تعیین می‌شود. برای کسب اطمینان خاطر از دید جامع از نیازمندی‌های امنیتی یک محصول (TOE)، زمانی که بر اساس این وابستگی‌ها و تشریک مساعی مولفه‌های در مستندات ST و PP نیازمندی‌ها برآورده می‌شود، وابستگی می‌تواند متقاعد کننده باشد. وابستگی‌ها باید زمانی که بسته‌ها طراحی می‌شوند در نظر گرفته شوند.

به عبارت دیگر: اگر مولفه (الف- با مولفه (ب) وابستگی داشته باشد، بدین معنا است که هرگاه مستند PP/ST شامل نیازمندی باشد که بر اساس مولفه (الف- طراحی شده باشد، باید در مستند PP/ST یکی از حالت‌های ذیل اتفاق بیافتد:

الف- نیازمندی امنیتی بر اساس مولفه (ب) است، یا

ب- نیازمندی امنیتی بر اساس یک مولفه که به شکل سلسله مراتبی بالاتر از مولفه (ب) قرار دارد است و یا

پ- توجیح کاملی باید باشد که چرا مستند PP/ST نیاز امنیتی را بر اساس مولفه (ب) طراحی نکرده است.

در حالت الف و ب، زمانی که نیازمندی امنیتی به دلیل وابستگی اضافه می‌شود، نیاز به یک سری عملیات کامل (تخصیص، تکرار، پایش، انتخاب) بر نیاز امنیتی به صورت یک رفتار معمول هستیم تا اطمینان حاصل شود که به شکل صحیح وابستگی برآورده شده است.

در حالت سوم، توجیه اینکه چرا نیازمندی امنیتی توسط مولفه ای برآورده نشده می‌تواند اینچنین بیان شود:

چرا وابستگی الزامی یا مفید نیست، یا

- وقتی وابستگی توسط محیط پیرامون محصول (TOE) بیان شده است، توجیه باید در این مورد باشد که چگونه اهداف امنیتی برای محیط عملیاتی موجب احصاء چنین وابستگی می‌شود، یا
- زمانی که وابستگی توسط مستند نیازمندی‌های کارکردی دیگری تحت الزامات رفتاری خاص خود بیان شده است (مانند SFRهای توسعه یافته، SFRهای ادغامی و غیره).

۳-۷ مولفه‌های توسعه یافته

در استاندارد ISO/IEC 15408 الزاما باید نیازمندی‌ها بر اساس مولفه‌های بیان شده در قسمت دوم و یا سوم تعریف شوند مگر در دو حالت زیر:

الف- هرگاه اهداف امنیتی برای یک محصول وجود داشته باشد که نتوان آن را منطبق بر نیازهای کارکردی بیان شده در قسمت دوم استاندارد بیان کرد، یا نیازهای ثالثی هم وجود داشته باشد(برای مثال: قوانین، استانداردها) که نتوان آن را منطبق بر نیازهای ضمانتی بیان شده در قسمت سوم استاندارد بیان کرد (برای مثال مسئله ارزیابی رمزنگاری)

ب- هدف امنیتی را می‌توان با مشکلات بسیار فراوان و/یا با پیچیدگی منطبق بر قسمت دوم یا سوم بیان کرد.

در هر دو مورد نویسنده PP/ST نیازمند تعریف مولفه‌های مورد نیاز خود است. این مولفه‌های جدید تحت عنوان مولفه‌های توسعه یافته نامیده می‌شود. یک تعریف مختصر از مولفه‌های توسعه یافته نیازمند این است که از مستند نیازمندی‌های کارکردی امنیت و مستند نیازمندی‌های ضمانت امنیت توسعه یافته مولفه‌ها توسعه یافته محتوی و مفهوم خود را اخذ کنند.

پس از تعریف مولفه‌های جدید، نویسنده PP/ST مولفه‌های توسعه یافته خود را بر مبنای یک یا چند SFR و SAR تعیین نموده و از آنها در همان مستندات یا دیگر SARs و SFRs استفاده کند. از این منظر فاصله ای بین SARs و SFRs که بر مبنی ISO/IEC 15408 طراحی شده اند و آن مستنداتی که بر مبنای مولفه‌های توسعه یافته طراحی شده است نمی باشد. با توجه به قسمت سوم استاندارد ISO/IEC 15408 تعریف مولفه توسعه یافته تحت APE_ECD و ASE_ECD صورت می‌گیرد.

۸ رخ‌نمون محافظتی و بسته‌ها

۸-۱معرفی

برای اینکه گروه‌های مصرف کنندگان و موسسات توان بیان نیازمندی‌های امنیتی خود را داشته باشند، و طراحی مستند هدف امنیتی تسهیل گردد، این قسمت از استاندارد ISO/IEC 15408 دو ساختار ویژه را معرفی می‌کند. بسته‌ها و رخ‌نمون محافظتی در ادامه این دو ساختار به تفصیل بیان می‌شود، بعلاوه در یک قسمت به چگونگی استفاده از این ساختارها پرداخته می‌شود.

۸-۲ بسته‌ها

بسته به مجموعه ای از نیازمندی‌های امنیتی گفته می‌شود. یک بسته همچنین

بسته کارکردی، که شامل تنها SFRs است ، یا

بسته ضمانت، که شامل تنها SARs است.

بسته ترکیبی، که شامل هم SARs و هم SFRs باشد مجاز نیست.

یک بسته می‌تواند توسط هر قسمت تشکیل شده باشد و هدف بر داشتن قابلیت استفاده مجدد این مستند است. برای دست یافتن به این هدف باید شامل نیازمندی‌هایی باشد که برای ادغام مفید و موثر باشند. بسته‌ها می‌تواند تحت ساختارهای بزرگتر قرار گیرد و به نوبه خود بسته‌های دیگری را ایجاد کنند، PPs و STs . در حال حاظر ضوابطی برای ارزیابی بسته‌ها وجود ندارد، بنابراین هر مجموعه از SFRs و SARs می‌تواند یک بسته باشد.

برای مثال بسته‌های ضمانتی می‌توان سطوح ضمانت EALs را ذکر نمود، که توسط قسمت سوم استاندارد ISO/IEC 15408 بیان شده اند. در این زمان هنوز هیچ بسته‌های کارکردی برای این نسخه از استاندارد ISO/IEC 15408 وجود ندارد.

۸-۳ رخنمون محافظتی

همانگونه که مستند هدف امنیتی ST به توصیف یک محصول خاص (برای مثال، دیواره آتش MinuteGap V18.5) می‌پردارد، یک مستند رخنمون محافظتی به توصیف یک محصول از یک رده و دسته خاص می‌پردازد (برای مثال، دیواره آتش‌ها). رخنمون محافظتی ممکن است بعنوان یک مستند پیش فرض و یک الگو در ارزیابی‌های مختلف برای تهیه انواع مستندات هدف امنیتی مورد استفاده قرار گیرد. جزئیات کامل از مستند PP در پیوست (ب) داده شده است.

به شکل عمومی، یک مستند هدف امنیتی ST به توصیف نیازمندی‌های یک محصول TOE پرداخته که توسط تولید کننده همان محصول طراحی و تکمیل می‌شود. در حالی که یک مستند PP به توصیف یک رده و دسته از محصولات می‌پردازد و می‌تواند توسط افراد زیر تهیه و تکمیل شود:

- اجتماعی از کاربران که به دنبال کسب توافق جمعی هستند تا مجموعه نیازمندی‌های یک رده از محصولات را تعیین کنند.
- یک توسعه دهنده محصول، یا یک گروهی از توسعه دهندگان که محصولات مشابه تولید می‌کنند برای ایجاد مجموعه حداقلهای الزامی که باید در همه محصولات از همان نوع رعایت شود
- یک دولت یا یک شرکت بزرگ برای توصیف نیازمندی‌های خود بعنوان قسمتی از فعالیت‌های فاز اکتساب در چرخه حیات تولید محصولات، می‌تواند به تولید PP بپردازد.

مستند PP محدوده مجازی را تعیین می‌کند که باید ST در آن محدوده تولید شود. (به بند ب-۵ مراجعه شود) مستند PP محدوده مجاز را اینگونه بیان می‌کند که:

- اگر مستند PP تاکید کامل بر رعایت الزامات به همان شکلی که بیان کرده داشته باشد، مستند ST باید به طور کامل تابع باشد.
- اگر مستند PP تاکید بر رعایت الزامات که بیان کرده داشته باشد، اما نه لزوما رعایت دقیق همه موارد ذکر شده، مستند ST می‌تواند از الزامات بیان شده به شکل کامل یا صورت مشابه تبعیت کند.

بعبارت دیگر مستند ST باید رفتاری منطبق یا مشابه رفتار تعیین شده در مستندPP داشته باشد، ومبتنی بر بیان خود مستند PP این رفتار تعیین می‌شود.

اگر مستند ST ادعایی مبنی بر مطابقت بر چندین PP را بیان داشته باشد، باید (همانطور که در بالا بیان شده است) نسبت به هر PP ذکر شده رفتاری دقیقا منطبق همان PP داشته باشد. بدین معنا که می‌تواند کاملا منطبق بر برخی از PPها باشد و نسبت به برخی دیگر فقط رفتاری مشابه داشته باشد.

توجه داشته باشید که مطابقت ST از PP یک مسئله بله خیر می‌باشد و مطابقت جزئی در استاندارد ISO/IEC 15408 مجاز نمی باشد. بنابراین مسئولیت نویسنده PP است که مستند را به گونه ای غیر پیچیده طراحی کند تا نویسندگان ST همانگونه که مورد نظر PP است مستندات خود را طرح کنند.

یک مستند ST معادل یا بسیار سختگیرانه تر از یک مستند PP است اگر:

- همه محصولات (TOEs) که الزامات بیان شده ST را برآورده می‌سازند نیازمندی‌های PP راهم برآورده سازند، و
- همه محیط‌های عملیاتی که منطبق با شرایط PP هستند با شرایط بیان شده ST هم منطبق باشند.

بعبارت ساده تر، مستند ST محدودیت‌هایی معادل آنچه در PP بیان شده حتی بیشتر از آن را بر TOE اعمال می‌کند و از طرف دیگر برای محیط عملیاتی محدودیت‌هایی معادل و یا کمتر از آنچه که در PP بیان شده است را بر محیط اعمال می‌کند.

در ذیل مهمترین مفاهیم که در محتوی ST بیان می‌شود ارائه شده است:

تعریف مسئله امنیتی[1]:

منظور از مطابقتی که در مستند ST است، این گونه است که مسئله امنیتی تعریف شده در ST معادل یا بسیار سختگیرانه تر از آن تعریفی است که در مستند PP بیان شده است. این بدین معنا است که:

- همه محصولاتی که مسئله امنیتی بیان شده در ST را برآورده ساخته است، قطعا باید مسئله بیان شده در مستند PP را برآورده ساخته باشد.
- همه محیط‌های عملیاتی که مسئله امنیتی بیان شده در مستند PP را برآورده می‌سازد، مسئله امنیتی مستند ST را برآورده می‌سازد.

اهداف امنیتی:

منظور از مطابقتی که در مستند ST است، این گونه است که اهداف امنیتی بیان شده در ST معادل یا بسیار سختگیرانه تر از آن تعریفی است که در مستند PP بیان شده است. این بدین معنا است که:

- همه محصولاتی که اهداف امنیتی بیان شده در ST را برآورده ساخته است، قطعا باید اهداف امنیتی بیان شده در مستند PP را برآورده ساخته باشد.
- همه محیط‌های عملیاتی که اهداف امنیتی بیان شده در مستند PP را برآورده می‌سازد، اهداف امنیتی مستند ST را برآورده می‌سازد.

اگر مطابق کامل از رخ‌نمون محافظتی مورد نظر باشد جملات زیر به کار می‌رود:

تعریف مسئله امنیتی: مستند ST باید شامل مسئله امنیتی بیان شده در مستند PP باشد، و همچنین می‌تواند از تهدیدهای بیان شده در مستندات بالادستی امنیت هر سازمان – مانند مستنداتOSPs)، برای شرح تکمیلی استفاده کرد، ولی نمی توان مفروضات اضافه تر از آنچه در PP بوده در نظر داشت.

اهداف امنیتی:مستند ST:

- می بایست شامل همه اهداف امنیتی در مورد TOE که در PP بیان شده باشد و همچنین می‌تواند برخی اهداف امنیتی اضافه تری را هم شرح کند.
- می بایست شامل همه اهداف امنیتی محیط عملیاتی باشد(با در نظر داشتن یک استثناء بیان شده در مطلب بعدی) اما هیچ هدف امنیتی اضافه تری ازمحیط نباید تعریف شود.

1- Security Problem Definition

ممکن است یک هدف امنیتی بیان شده برای محیط عملیاتی در مستند PP خود یک هدف امنیتی برای TOE در مستندST باشد. به این مسئله باز-تخصیص گفته می‌شود. هرگاه یک هدف امنیتی بازتخصیص شود، باید به طور واضح و کامل تعیین شود که چه قسمتی ضروری و چه قسمتی اضافی است.

پ)نیازمندی‌های امنیتی:

مستند ST باید شامل همه SARs و SFRs باشد، اما ممکن است مدعی وجود مستندات اضافه تر یا قوی تری از SARs و SFRs شود. تکمیل عملیات در مستند ST باید همانگونه که در مستند PP انگاره شده است، بیان شود، و یا اینکه کمی نیازمندی‌ها محدود تر استفاده می‌شود (عملیات پایش بکار گرفته می‌شود).

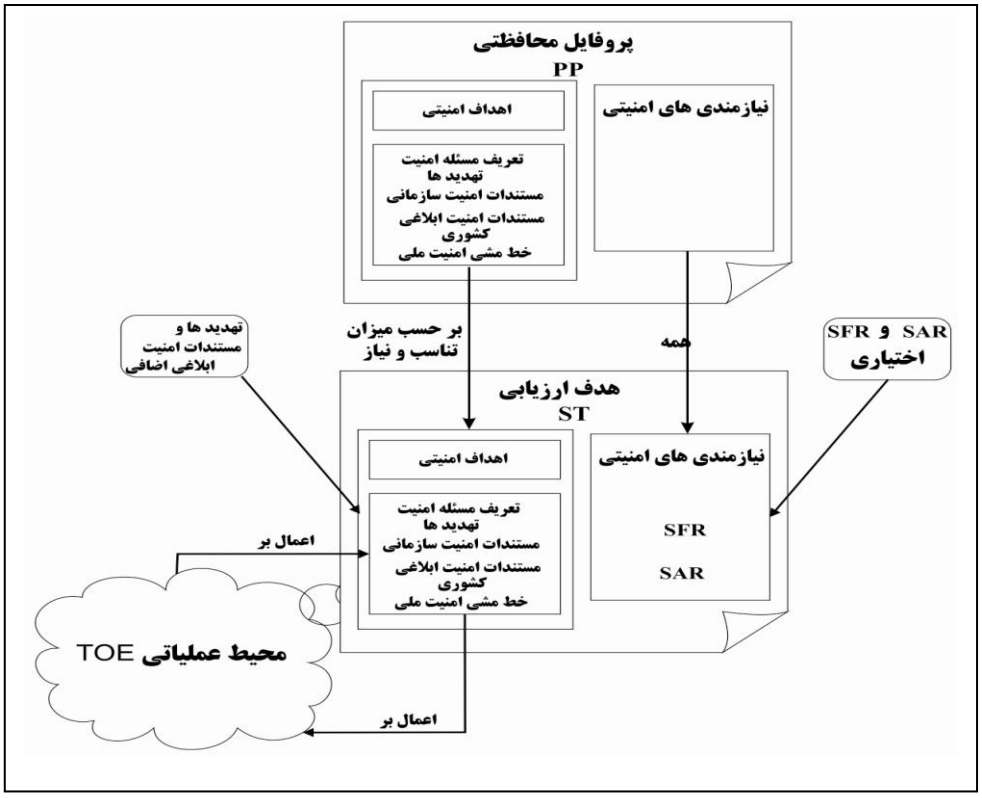
هرگاه انطباق قابل اثبات صورت گرفته باشد ، الزامات زیر اعمال شده اند:

- مستند ST باید اثبات کند که چرا معادل یا محدودتر از مستند PP تهیه شده است.
- اثبات تطابق، نویسنده PP را مجاز می‌دارد تا مسائل امنیتی معمول تری را حل کند و مستندات راهنمای کلی و عمومی برای شفاف سازی نیازمندی‌های ضروری تهیه و ارائه کند.

ارزیابی PP اختیاری است. ارزیابی این مستند از طریق اعمل ضوابط کلاس APE که در قسمت سوم استاندارد ISO/IEC 15408 بیان شده است تعیین می‌شود. هدف چنین ارزیابی نشان دادن کامل بودن مستند PP است. که می‌توان کامل بودن را به معنای مناسب بودن از نظر فنی، قابلیت استفاده بعنوان یک مستند الگو برای تهیه مستندات ST و یا PP دیگر تعریف کرد.

بر این اساس یک مستند PP ارزیابی شده دو مزیت زیر را دارد:

- ریسک وجود خطا در این مستند و همچنین موارد مبهم و یا ذکر نشده در این مستند ارزیابی شده بسیار کمتر است. اگر هر مشکلی در یک PP وجود داشته باشد و درزمان نگارش و یا ارزیابی هر مستند ST به وجود این گونه خطاها پی برده شود، زمان زیادی برای حل این مسئله از دست خواهد رفت.
- ارزیابی هر PP/ST جدید می‌تواند از نتایج ارزیابی مستندات PP ارزیابی شده استفاده مجدد کند، این مسئله منجر به کاهش تلاش و هزینه در ارزیابی هر مستند PP/ST جدید خواهد شد.



۸ـ٤ استفاده از مستندات PP و بسته‌ها

هرگاه هر مستند ST ادعایی مبتنی بر انطباق با یک یا چند بسته یا رخ‌نمون محافظتی را داشته باشد، ارزیابی آن مستند (علاوه بر دیگر ویژه‌های آن) به معنای به اثبات رساندن تطابق واقعی آن با مستندات ادعا شده است. جزئیات این تعیین تطابق در پیوست الف ذکر شده است.

فرایند زیر مجاز است:

الف- هر سازمان که به دست آوردن نوع خاصی از محصول امنیتی فنآوری اطلاعات را جستجو می‌کند، باید نیازمندی‌های امنیتی خود را در قالب مستند PP توسعه دهد و مستند ارزیابی شده خود را منتشر سازد.

ب- هر توسعه دهنده با در دست داشتن این مستندات PP، مستند ST معادلی را طراحی می‌کند و ادعای تطابق این مستند با PPهای منتشر شده را بیان می‌دارد.

پ) توسعه دهنده با ساخت محصول (یا استفاده از محصولات موجود)، ارزیابی محصول با مستند ST تایید شده را انجام می‌دهد.

نتیجه این فرایند این است که تولید کننده می‌تواند محصولی منطبق با نیازمندی‌های هر سازمان تولید کند، هر سازمان می‌تواند محصولی مطابق با آنچه واقعا نیاز داشته و اعلام کرده تهیه کند. به همین ترتیب می‌تواند در مورد بسته‌ها هم اتفاق بیافتد.

۸ـ٥ استفاده از رخ‌نمون‌های محافظتی چند گانه

در استاندارد ISO/IEC 15408 تهیه مستندات PP منطبق بر مستندات PP دیگر و همچنین تهیه مجموعه مستندات زنجیره ای PP که هرکدام بر مبنای مستند قبلی تهیه شده باشند را مجاز می‌دارد.

برای نمونه، اگر فردی قصد تهیه یک مستند PP برای مدار یکپارچه داشته باشد، و یک مستند PP برای سامانه عامل کارت هوشمند Smart Card OS می‌تواند این ساختار را تحت قالب مستند رخ‌نمون محافظتی کارت هوشمند ارائه دهد به گونه ای که منطبق برای هر دو نیاز باشد. از سوی دیگر فرد دیگر می‌تواند رخ‌نمون محافظتی تهیه کند برای کارت هوشمند در حمل و نقل عمومی بر مبنای رخ‌نمون محافظتی کارت هوشمند و

رخ‌نمون محافظتی. سرانجام هر توسعه دهنده می‌تواند مستند ST تهیه کند برای کارت‌های هوشمند استفاده شونده در حمل نقل عمومی که از همه این مستندات PPعنوان شده استفاده کند.

۹-نتایج ارزیابی

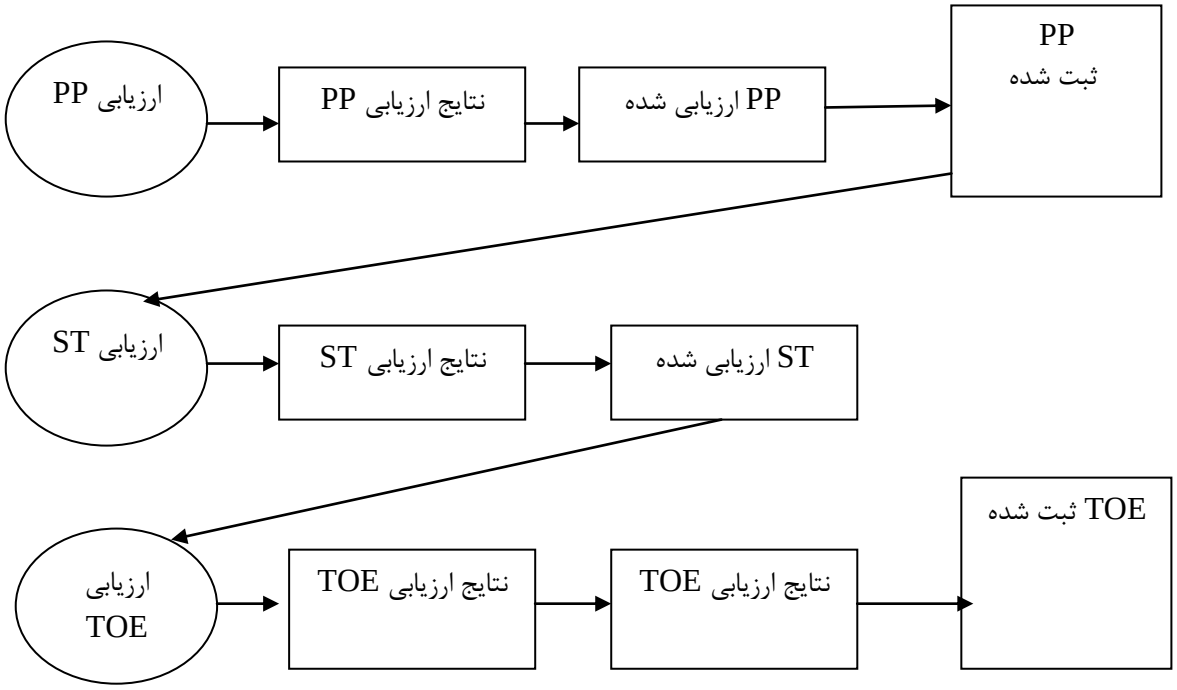
۹-۱ مقدمه

این بند، نتایج مورد نظر حاصل از ارزیابی PP و TOE/ST بر اساس ISO/IEC 18045 را ارائه می‌کند.

• ارزیابی PP منجر به ایجاد کاتالوگ‌هایی از PPهای ارزیابی شده می‌شود.

• ارزیابی ST منجر به نتایج متوسطی که در چارچوب کاری ارزیابی TOE استفاده شده است، می‌شود.

• ارزیابی TOE / ST منجر به ایجاد کاتالوگ‌هایی از TOE ارزیابی شده می‌شود. در بسیاری از موارد این کاتالوگ‌ها مراجعه خواهند کرد به محصولات IT که TOE از آنها ، ونه از یک TOE خاص مشتق شده است. بنابراین، وجود یک محصول فناوری اطلاعات در یک کاتالوگ نباید به این معنی باشد که کل محصول IT، به جای میزان واقعی ارزیابی TOE / ST که توسط ST تعریف شده است ارزیابی شده است.. مراجعه کنید به کتابشناسی برای نمونه‌هایی از کاتولوگ‌ها.



شکل ۵-نتایج ارزیابی

اهداف ارزیابی ممکن است بر اساس بسته‌ها،PPهای محافظت شده یا محافظت نشده باشند-در هر صورت این الزامی نیست، به طوری که اهداف ارزیابی اصلا میتواند بر هیچ اساس بنا شده باشند.

ارزیابی باید منجر به نتایج هدفمند و قابل تکراری شود که بتوان آن را به عنوان مدرک درنظر گرفت حتی اگر هیچ معیار کاملا هدفمندی جهت ارائه نتایج ارزیابی امنیت IT وجود نداشته باشد. وجود مجموعه‌ای از معیارهای

ارزیابی، پیش شرط ضروری برای ارزیابی می‌باشند که باعث ایجاد نتایج معنادار شده و مبنایی فنی را برای شناسایی متقابل نتایج میان مراجع ارزیابی فراهم می‌کنند. اما کاربرد معیار، شامل مؤلفه‌های عینی و ذهنی بوده و به همین دلیل است که درجه بندی دقیق و کلی امنیت IT، عملی نمی‌باشد.
درجه‌بندی که درارتباط با این استاندارد ملی ایجاد شده، نتایج نوع خاصی از بررسی‌های ویژگی امنیتی TOE را نشان می‌دهد. چنین درجه بندی، سازگاری را برای استفاده در هر محیط کاربردی خاصی ضمانت نمی‌کند. تصمیم جهت پذیرش TOE برای استفاده در محیط کاربردی خاص، بر مبنای توجه به بسیاری از مباحث امنیتی ازجمله نتایج ارزیابی می‌باشد.

۹-۲ نتایج ارزیابی PP

این استاندارد ملی شامل معیار امنیتی می‌باشد که به ارزیاب این امکان را می‌دهد تا کامل بودن، سازگار بودن و از نظر فنی بی‌عیب بودن و بنابراین مناسب بودن آن را جهت استفاده به‌عنوان بیانیه الزامات برای TOE قابل ارزیابی، اظهار کند.
ارزیابی PP باید منجر به پذیرش/ عدم پذیرش دستور شود. PP که مورد قبول قرار گرفته باید جهت ثبت در فهرست، واجد شرایط باشد.

۹-۳ نتایج ارزیابی ST/TOE

قسمت ۳ از این استاندارد ملی شامل معیارهای ارزیابی است که ارزیاب موظف است به منظور تعیین اینکه آیا اطمینان کافی وجود دارد که TOE، SFRs درST رابرآورده می‌کند،مشورت کند. بنابراین، بررسی TOE باید منجر به بیانیه پاس / خرابی برای ST شود.اگر نتیجه هر دو ST و ارزیابی TOE پاس باشد، محصول زیر بنایی واجد شرایط لازم برای ورود به در رجیستری است.نتایج حاصل از ارزیابی باید همچنین شامل "ادعای انطباق" همان طور که در ۹-۴ تعریف شده است، باشد.
ممکن است که نتایج ارزیابی پس از آن در یک فرآیند صدور گواهینامه استفاده شوند، اما این فرآیند صدور گواهینامه خارج از محدوده این استاندارد ملی می‌باشد.

۹-٤ ادعای تطابق

نتایج تطابق، منبع گردآوری الزاماتی که از طریق TOE یا PP برآورده و ارزیابی روی آن انجام شده را نشان می‌دهد. این نتیجه تطابق، نسبت به قسمت ۲ این استاندارد ملی (الزامات عملیاتی)، قسمت ۳ این استاندارد ملی (الزامات تضمین) و در صورت قابل اجرا بودن، برای مجموعه از پیش تعیین شده‌ای از الزامات (برای مثال، EAL، پروفایل محافظتی) ارائه می‌شود.
نتیجه تطابق، دربرگیرنده یکی از موارد زیر می‌باشد:
الف- تطابق این استاندارد ملی- قسمت۲[1]: در صورتی که الزامات عملیاتی تنها بر مبنای مؤلفه‌های عملیاتی در این استاندارد ملی– قسمت ۲ باشند، PP یا TOE، با قسمت ۲ این استاندارد ملی تطابق دارند..

1- ISO/IEC 15408-2 conformant

ب- **توسعه یافته این استاندارد ملی-قسمت[1]۲:** PP یا TOE این استاندارد ملی-قسمت ۲ در صورتی توسعه یافته می‌باشدکه، الزامات عملیاتی تنها بر مبنای مؤلفه‌های عملیاتی موجود در این استاندارد ملی-قسمت ۲ باشند.

و همچنین یکی از موارد زیر:

الف- تطابق این استاندارد ملی-قسمت ۳: در صورتی که الزامات تضمین تنها بر مبنای مؤلفه‌های تضمین در این استاندارد ملی-قسمت ۳ باشند، PP یا TOE، با این استاندارد ملی-قسمت ۲ تطابق دارند.

ب- توسعه یافته این استاندارد ملی-قسمت ۳: در صورتی PP یا TOE، قسمت ۳ این استاندارد ملی توسعه یافته می‌باشد که، الزامات تضمین شامل الزاماتی باشد که در این استاندارد ملی-قسمت ۳ وجود نداشته باشد.

علاوه‌براین، نتیجه تطابق ممکن است شامل بیانیه‌ای باتوجه به الزامات تعیین شده باشد، در این‌صورت، بیانیه شامل موارد زیر می‌باشد:

الف- تطابق عنوان بسته[2]:در صورتی که الزامات (عملیاتی یا تضمین) شامل کلیه مؤلفه‌ها در بسته‌های فهرست شده به عنوان قسمتی از نتیجه تطابق باشند، PP یا TOE با بسته عملیاتی یا تضمین از پیش تعیین شده، (مانند EAL) هماهنگ می‌باشد.

ب- عنوان بسته اضافه شده[3]: در صورتی که الزامات (عملیاتی یا تضمین) مجموعه‌های مناسبی از کلیه مؤلفه‌ها در بسته‌های فهرست شده به عنوان قسمتی از نتیجه تطابق باشند، PP یا TOE با بسته عملیاتی یا تضمین از پیش تعیین شده (مانند، EAL) یکی می‌باشد.

در نهایت، نتایج تطبیق همچنین ممکن است شامل بیانیه‌ای باتوجه به پروفایل‌های محافظتی باشد که شامل موارد زیر می‌شود:

الف- تطابق PP[4] : TOE، PPهای خاصی را که به عنوان قسمتی از نتایج تطابق فهرست شده‌اند را ایجاد می‌کند.

۹-۵ استفاده از نتایج ارزیابی TOE / ST

هنگامی که ST وTOE مورد بررسی قرار گرفته اند، صاحبان دارایی می‌تواند تضمین شوند (همان طور که تعریف شده در ST) که TOE، همراه با محیط عملیاتی، در مقابل تهدیدات.نتایج ارزیابی ممکن است توسط مالک دارایی در تصمیم گیری که آیا برای قبول خطر افشای دارایی‌ها به تهدید استفاده می‌شود.

با این حال، مالک دارایی باید با دقت چک کنید که آیا:

- مشکل تعریف امنیت در ST منطبق با مشکل امنیتی از مالک دارایی است؛
- محیط عملیاتی از صاحب دارایی مطابق (و یا می‌توان به مطابقت) به اهداف امنیتی برای محیط عملیاتی در ST باشد.

1- ISO/IEC 15408-2 extended

2 - Package name conformant

3 - Package name augmented

4 - pp conformant

اگر هر کدام از این حالتها وجود نداشته باشد، TOE ممکن است مناسب اهداف مالکان دارایی نباشد.
علاوه بر این، هنگامی که TOE ارزیابی شده در حال بهره برداری است ، هنوز هم ممکن است که خطاهای ناشناخته یا آسیب پذیری‌ها در TOE ممکن است ظاهر شود. در این صورت، توسعه دهنده ممکن است TOEرا (برای ترمیم آسیب پذیری‌های) اصلاح کند و یا ST را به منظور حذف آسیب پذیری از حوزه ارزیابی، تغییر دهد. در هر صورت، نتایج ارزیابی‌های قدیمی ممکن است دیگر معتبر نباشد.
اگر لازم باشد که اطمینان مجدد حاصل شود، ارزیابی مجدد مورد نیاز است. این استاندارد ملی ممکن است برای این ارزیابی مجدد استفاده شود، اما مراحل دقیق برای ارزیابی مجدد در خارج از محدوده این استاندارد ملی می‌باشد.

پیوست الف

(اطلاعاتی)
ویژگی اهداف امنیتی

الف-۱ هدف و ساختار این پیوست

این پیوست شرح مفاهیم مستند هدف امنیتی است. این پیوست ضوابط مربوط به کلاس ASE را معرفی نمی کند، و این ضوابط در قسمت سوم استاندارد ISO/IEC 15408 مطرح شده است.

این پیوست در چهار محور اساسی زیر بحث می‌کند:

الف- مستند هدف امنیتی شامل چه‌ها (What) باید(Must) باشد. الزامات اجباری که در مستند ارزیابی باید قرار گیرد، روابط بین این قسمت‌ها با ذکر مثال‌هایی بیان می‌شود.

ب- چگونه (HOW) باید(Should) از مستند هدف امنیتی استفاده کرد. این قسمت به توصیف چگونگی استفاده از مستند هدف امنیتی و برخی سئوالات که مستند ارزیابی می‌تواند پاسخ دهد، بیان می‌شود.

پ)مستندهای هدف امنیتی با حداقل سطح ضمانت می‌کنند. مستندهای هدف امنیتی که محتوی کاهش یافته ای دارند.

ث)اظهار ادعا به شکل استاندارد. این مسئله که چگونه یک نویسنده مستند هدف امنیتی می‌تواند ویژگی‌های خاصی که محصول (TOE) برآورده ساخته است را بیان کند.

الف-۲مندرجات اجباری در مستند هدف امنیتی

شکل زیر همه مندرجات الزامی که مستند هدف امنیتی منطبق بر مفاد قسمت سوم استاندارد ISO/IEC 15408 باید داشته باشد را به تصویر کشیده است. این شکل می‌تواند یک نقشه اجمالی از ساختار مستند هدف امنیتی در نظر گرفته شود هرچند که هر ساختار دیگر (ضمن رعایت الزامات قسمت سوم ISO/IEC 15408) مجاز می‌باشند. برای مثال، اگر الزامات امنیتی بسیار زیادی وجود داشته باشد، می‌توان قسمتی از این الزامات را در یک پیوست در مستند هدف امنیتی قرار داد به جای اینکه همه این حجم انبوه مطالب را در قسمت الزامات امنیتی مستند هدف امنیتی قرار داده شود. قسمت‌های مجزای یک مستند هدف امنیتی و محتوی آنها به شکل خلاصه در زیر مطرح شده اند. یک مستندهدف امنیتی به طور معمول شامل:

الف-مقدمه، شامل خلاصه کوتاه و توصیفی از سه سطح مختلف محصول به شکل انتزاعی است.

ب- ادعای تطبیق، قسمت‌هایی از ST که منطبق بر هر PP (ها) یا بسته (ها) هستند در این قسمت نشان داده می‌شود.

ج) تعریف مسئله امنیت، نشان دهنده تهدیدها، OSPs، و همه مفروضات امنیتی را نشان می‌دهد.

د)اهداف امنیتی، نشان دهنده این است که چگونه برآورده شدن یک مسئله امنیتی توسط تقسیم آن به شکل اهداف امنیتی برای محصول و محیط انجام می‌شود.

ه)تعریف مولفه‌های اضافی (اختیاری)، هر گاه مولفه جدید (علاوه برآنچه در قسمت دوم و سوم ISO/IEC 15408 بیان شده است) تعریف شود، این مولفه‌های جدید باید تحت قالب مولفه‌های عملکردی امنیت و مولفه‌های ضمانتی امنیت اضافی تعریف شوند.

و) الزامات امنیتی، درواقع تفسیری از یک هدف امنیتی برای محصول در قالب یک زبان استاندارد است. این زبان استاندارد درون مستندات SFRs و SARs است.

ز) خلاصه توصیف محصول، شرح چگونگی اعمال SFRs به درون محصول است.

مستند هدف امنیتی با حداقل سطح ضمانت با مندرجات کاهش یافته هم وجود دارد که در انتهای این پیوست توضیح داده می‌شود، بطور کلی این پیوست یک مستند هدف امنیتی کامل و جامع را در نظر می‌گیرد.

الف-۳ استفاده از مستند هدف امنیتی

الف-۳-۱ چگونه یک مستند هدف امنیتی باید استفاده شود.

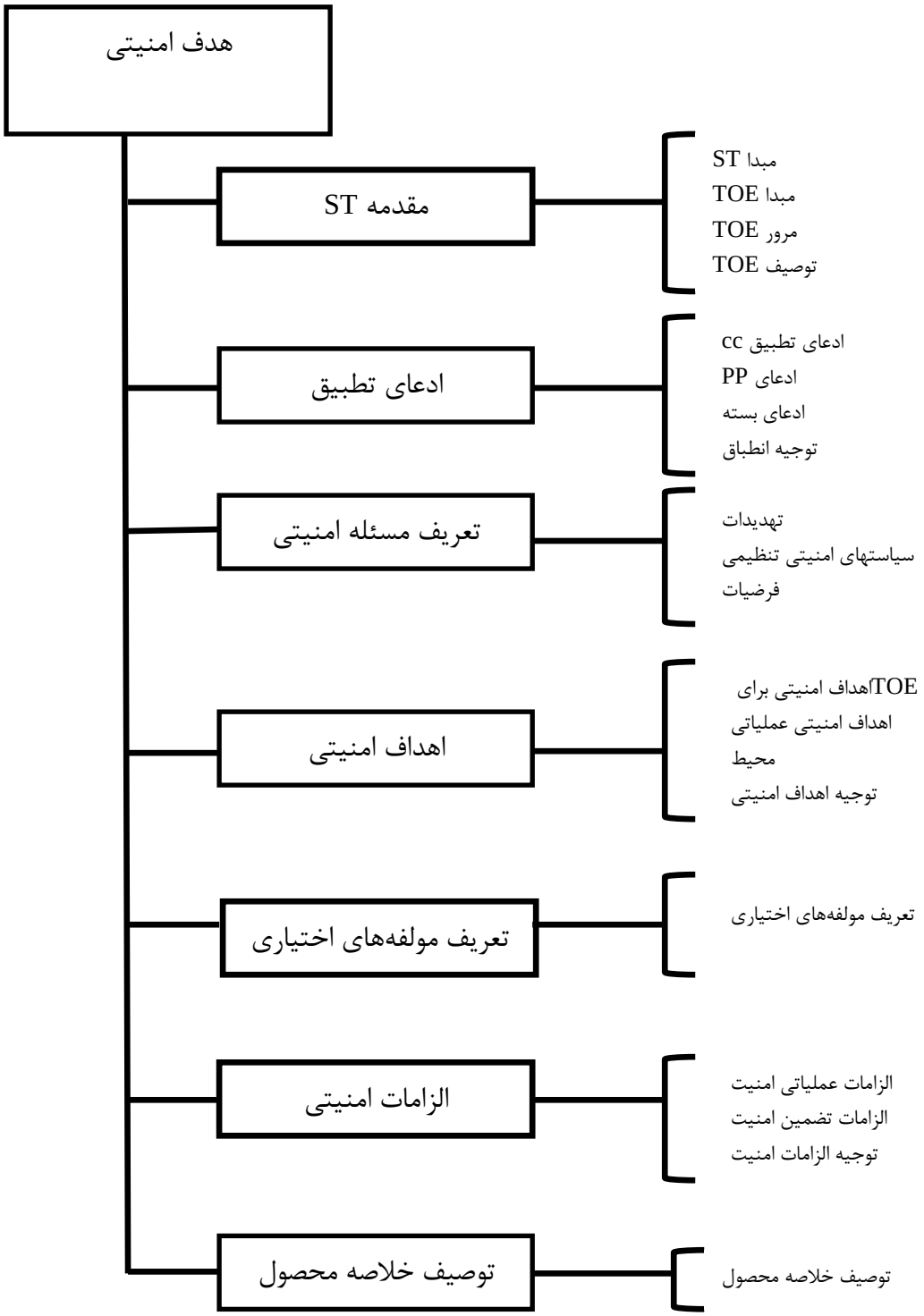
هر مستند ST بطور عمومی دو وظیفه اصلی را برعهده دارد:

- مستند هدف امنیتی قبل و در حین اجرای ارزیابی اینکه "چه چیزی باید ارزیابی شود" را شرح می‌دهد. بر اساس این وظیفه، مستند هدف امنیتی اصلی ترین معیار است که توسعه دهنده و ارزیاب بر سر خصوصیاتی از محصول که باید ارزیابی شود و اساسا بر هدف امنیتی ، توافق می‌کنند. صحت و جامعیت فنی مهمترین مسئله در این وظیفه است.
- مستند هدف امنیتی پس از ارزیابی "چه چیزی ارزیابی شده است" را شرح می‌دهد. منطبق این وظیفه، مستند هدف امنیتی اساسی ترین محور توافق برای توسعه دهنده، بازاریاب و مشتریان باقوه محصول است. این مستند خصوصیات امنیتی محصول را به شکل کاملا دقیق در یک سطح انتزع بیان می‌کند، مشتریان بالقوه محصول مبتنی بر آنچه ارزیابی شده است می‌توانند بر صحت ویژگیها اطمینان کنند.سهولت استفاده و قابلیت فهم مهمترین خصیصه در این قسمت می‌باشد.

الف -۳-۲ چگونه یک مستند هدف امنیتی نمی بایست استفاده شود

مستند هدف امنیتی نباید به دو شکل زیر مورد استفاده قرار گیرد:

- شرح با جزئیات زیاد، مستند هدف امنیتی برای بیان خصوصیات امنیتی در سطوحی از انتزاع طراحی شده است. این مستند باید، به شکل عمومی بیان شود و نباید برای مثال از جزئیات الگوریتم، پروتکل خاص و /یا مکانیسم خاص توصیف با جزئیات بیان شود.
- شرح کامل، مستند هدف امنیتی برای ارائه شرح کلی و انتزاعی از امنیت محصول طراحی شده نه توصیف کل خصیصه‌های محصول. بجزء همه مواردی که با امنیت سروکار دارند، برای مثال خصیصه‌هایی چون ، قابلیت اجرای درونی، اندازه فیزیکی یا وزن یا حتی ولتاژ مورد نیاز و غیره نباید جزئی از مستند هدف امنیتی باشند. بدین معنا که در شکل کلی، یک مستند هدف امنیتی ممکن است قسمتی از یک توصیف جامع برای محصول باشد ولی نباید خودش توصیف جامعی از محصول ارائه دهد.



شکل الف-۱:محتوای هدف امنیتی

الف-٤معرفی هدف امنیتی ASE_INT

این قسمت از ST، به معرفی محصول در سه سطح از انتزاع به شکل خلاصه می‌پردازد:

الف- مستندات مرجع ST و محصول، که منجر به شناسایی مفاد ST و محصول گردد.

ب-مروری بر محصول، توصیف خلاصه ای از محصول

پ)شرح محصول، توضیحی با جزئیات بیشتری در خصوص محصول

الف-٤-١مستندات مرجع ST و محصول

یک مستند هدف امنیتی باید به صورت شفاف مراجعی را معرفی کند که ویژه آن مستند است. بصورت عمومی باید، عنوان، نسخه، نویسنده و تاریخ نشر مستندات عنوان شود. بعنوان مثال: "MauveRAM Database ST, version 1.3,MauveCorp Specification Team, 11 October 2002".

در مستند هدف امنیتی باید مراجعی برای شناساسیی مطابقت ادعاهای مطرح شده برای محصول در این مستند بیان شود. به طور عمومی برای هر مرجع باید، نام توسعه دهنده، نام محصول، شماره نسخه محصول بیان شود. بعنوان مثال: "MauveCorp MauveRAM Database, V2.11". هر محصول ممکن است چندین بار توسط توسط مشتریان مختلف ارزیابی شود، بنابراین مستندات اهداف ارزیابی متفاوتی برای یک محصول ممکن است وجود داشته باشد و این مرجع الزاما در همه این مستندات یکسان نیست.

اگر محصول TOE، از یک یا چند محصول شناخته شده تشکیل شده باشد، انعکاس این مسئله بعنوان مراجع محصول البته با ارجاع به نام محصولات، مجاز می‌باشد. هرچند این مسئله، در شرایطی که قسمت‌های مهم یا عملکرد امنیت که در ارزیابی مورد نظر نمی باشند، نباید برای گمراه کردن مشتریان استفاده شود، ولی باز هم عدم ذکر این موارد مجاز نیست.

مراجع ST و TOE روند مرتب سازی و شناسایی مراجع ST و TOE را تسهیل می‌کند و در مجموع شامل فهرست خلاصه ای از محصولات و TOEهای ارزیابی شده هستند.

الف-٤-٢ مرور بر TOE

این قسمت با هدف کمک به مشتریان بالقوه ای است که از فهرست محصولات ارزیابی شده در جستجوی محصولی هستند که نیاز آنها را برآورده سازد و از سوی دیگر با تجهیزات مورد نظر مشتریان از نظر سخت افزاری و نرم افزاری و میان افزاری مطابقت دارد. به طور معمول این قسمت شامل چند پاراگراف است.

به همین دلیل، این قسمت توصیف خلاصه ای از موارد استفاده محصول و مهمترین خصیصه‌های امنیتی، نوع محصول و نیازمندی‌های تجهیزاتی (سخت افزار، نرم افزار، لخت افزار) به جز محصول مورد ارزیابی (NON - TOE)آن را توصیف می‌کند.

الف-٤-٢-١ موارد استفاده و مهمترین خصوصیت ویژه TOE

در این قسمت، ایده کلی از آن چه توانایی محصول از نظر امنیت است، و آن استفاده ای که در حوزه امنیت از محصول می‌شود ارائه می‌گردد. این قسمت برای مشتریان بالقوه نوشته می‌شود، توصیف خصیصه‌های مهم امنیتی و نوع استفاده آن در عملیات کسب و کار و تجارت به زبانی که قابل فهم برای مشتری باشد انجام می‌شود.

بعنوان مثال: "MauveCorp MauveRAM Database, V2.11". یک پایگاه داده چند کاربره است که باید بعنوان تجهیزات شبکه ای استفاده شود. ۱۰۲۴ کاربر به طور همزمان قابلیت استفاده از آن را دارند. این محصول قابلیت احراز هویت زیست سنجی، پسورد و Token را می‌دهد و از ازبین رفتن اطلاعات به شکل تصادفی جلوگیری می‌کند. قابلیت بازگشت به عقب هزار تراکنش را داراست. خصیصه‌های ممیزی آن در سطح بسیار

بالایی قابل پیکربندی است و همچنین قابلیت انجام ممیزی با جزئیات بر برخی کاربران یا تراکنش‌ها را در حالی که از حریم خصوصی باقی تراکنش‌ها و کاربران حفاظت کند را ارائه می‌دهد.

الف ـ٤ـ٢ـ٢ نوع TOE

در قسمت مرور بر TOE باید بصورت عمومی نوع TOE مشخص شود، مانند اینکه: دیوار آتش، VPN-Firewall، کارت هوشمند، مودم رمزنگار، اینترانت، وب سرور، پایگاه داده، شبکه محلی و سراسری با پایگاه داده و وب سرور و غیره.

اصطلاح NONE برای مواردی است که TOE از انواع شناخته شده در دسترس نباشد.

در برخی موارد نوع محصول TOE ممکن است موجب گمراهی مشتریان شود. مانند:

- عملکرد مطمئنی از TOE مورد توقع باشد در حالی که این عملکرد توسط خود محصول ارائه نشود مانند:
  - یک ATM-Card، که هیچ عملیات تشخیص و اهراز هویت را نداشته باشد.
  - یک دیواره آتش که از پروتکل‌های عمومی استفاده کند.
  - یک PKI-Type، که عملیات فسخ و بازستانی گواهی شده را ارائه ندهد.
- ممکن است اجرای مطمئن عملیات توسط یک محصول در محیط مورد توقع باشد، در حالی که خود محصول بر اساس نوع آن چنین قابلیتی را واقعا ارائه نکند مانند:
- یک سامانه رایانه شخصی، که توان اجرای عملیات امن را ندارد مگر اینکه در شبکه نباشد و هیچ ورودی از نوع فلاپی، سی دی و دی وی دی و غیره نداشته باشد.
- یک دیواره آتش، قادر به اجرای عملیات به شکل امن نیست مگر اینکه ارتباطات همه کاربران از این پودمان عبور کند.

الف‌ـ٤ـ٢ـ٣ نیازمندی‌های سخت افزاری/نرم افزاری/لخت افزاری غیر از هدف مورد ارزیابی

هرچند که بسیار از محصولات مورد ارزیابی به هیچ محصول فنآوری دیگری تکیه ندارند، ولی بسیاری از محصولات مورد ارزیابی (خصوصا نرم افزارها) به صورت اضافی به برخی از تجهیزات وابسته هستند. بعبارت دیگر، در قسمت مرور TOE باید این نوع وابستگی‌ها بیان شود. شرح کامل و با جزئیات دقیق همه تجهیزات نرم افزاری/سخت افزاری/لخت افزاری مورد نظر نیست، ولی مشتریان بالقوه باید اطلاعات مکفی از تجهیزات فنآوری پیرامون محصول ارزیابی شده داشته باشند.

برای مثال:

- یک رایانه رومیزی استاندارد (PC)، با پردازنده 1GHz، حافظه اصلی 512MB، که سامانه عامل Yaiza نسخه 3.0 که به نسخه 6b یا c یا ۷ و یا حتی نسخه 4.0 بروزرسانی شده است.
- یک رایانه رومیزی استاندارد (PC)، با پردازنده 1GHz، حافظه اصلی 512MB، که سامانه عامل Yaiza نسخه 3.0 که به نسخه 6b یا c یا ۷ و یا حتی نسخه 4.0 بروزرسانی شده است و کارت نگاره WonderMAgic 1.0 با ست درایور WM 1.0
- یک رایانه رومیزی استاندارد (PC)، با سامانه عامل Yaiza نسخه 3.0 یا بالاتر.
- یک مدار مجتمع CleverCard SB2067

- یک مدار مجتمع CleverCard SB2067 به همراه سامانه عامل کارت هوشمند QuickOS V2.0

الف-٤-٣ توصیف TOE

این قسمت به شرح خلاصه محصول مورد ارزیابی می‌پردازد که ممکن است چندین صفحه باشد. این قسمت به ارزیابان و مشتریان بالقوه امکان شناسایی توانمندی‌های امنیتی محصول مورد ارزیابی را می‌دهد، به گونه ای که جزئیات بیشتری نسبت به قسمت قبل باید در این قسمت ذکر شود. این قسمت ممکن است به توضیح کابردهای گسترده تری که متناسب محصول مورد ارزیابی است، بپردازد.

این قسمت در خصوص محدوده فیزیکی محصول مورد ارزیابی بحث می‌کند. فهرستی از همه محصولات سخت افزاری، نرم افزاری و میان افزاری و قسمت‌های راهنما که مجموعا محصول مورد ارزیابی را تشکیل می‌دهند. این قسمت باید سطحی از جزئیات را به گونه ای که برای خوانندگان معمولی قابل فهم باشد ارائه کند.

این قسمت در خصوص محدوده منطقی محصول مورد ارزیابی نیز بحث می‌کند، این قسمت باید سطحی از جزئیات خصیصه‌های منطقی امنیت را به گونه ای که برای خوانندگان معمولی قابل فهم باشد ارائه کند. انتظار می‌رود که جزئیات بیان شده در این قسمت نسبت به قسمت بیان مشخصه‌های اصلی امنیت بیشتر باشد.

اصلی ترین ویژگی قسمت توصیف منطقی و فیزیکی این است که TOE به گونه ای شرح داده شود که هیچ شکلی در خصوص قسمتهای مطمئن و خصیصه‌های محصول باقی نماند. بخصوص زمانی که محصول مورد ارزیابی در تجهزات غیر هدف امنیتی به گونه ای آمیخته باشد که نتوان تفکیکی بین این دو قائل شد.

مثالهایی برای محصولات درهم آمیخته با تجهیزات فنآوری:

- هدف مورد ارزیابی یک پردازنده رمزنگار از مدار یکپارچه کارت هوشمند باشد، به جای اینکه کل مدارد هدف مورد ارزیابی باشد.
- هدف مورد ارزیابی کل مدار یکپارچه کارت هوشمند باشد بجز پردازنده رمزنگاری آن
- هدف مورد ارزیابی قسمت مترجم آدرس شبکه در دیواره آتش MinuteGap V18.5 باشد.

الف-٥ ادعای انطباق

این قسمت مستند هدف امنیتی چگونگی تطبیق مستند را شرح می‌دهد. که انطباق‌ها در سه حالت می‌تواندصورت گیرد:

- انطباق با قسمت دوم و سوم استاندارد
- انطباق با رخ‌نمون‌های محافظتی
- انطباق با بسته‌ها

شرح اینکه یک مستند هدف امنیتی چگونه منطبق مفاد ISO/IEC 15408 است در دو قسمت صورت می‌گیرد: نسخه ای از استاندارد ISO/IEC 15408 که استفاده می‌شود و استفاده یا عدم استفاده مستند هدف امنیتی از نیازمندی‌های اضافی

شرح تطبیق مستند هدف امنیتی با رخ‌نمون‌های محافظتی و بسته‌ها به این معنا است که، مستند هدف امنیتی فهرست بسته‌هایی که ادعای تطبیق برآنها شده است را ارائه می‌کند.

الف ـ٦ تعریف مسئله امنیتی ASE_SPD

الف-٦-١معرفی

این قسمت به معرفی مسئله امنیتی که عنوان شده است می‌پردازد. فرایند تعریف مسئله امنیتی در محدوده استاندارد ISO/IEC 15408 نمی گنجد.

هرچند باید در نظر داشت که ثمره نتایج ارزیابی‌ها قویا وابسته به مستند ST است و ثمره طراحی یک مستند هدف امنیتی قوی وابسته به تعریف مسئله امنیتی می‌باشد. بنابراین استفاده از منابع کافی و فرایندهای مناسب و کارا برای تحلیل و تعیین دقیق و صحیح از مسئله امنیتی اغلب ارزنده و گرانبها است.

توجه داشته باشید که برمبنای قسمت سوم استاندارد ISO/IEC 15408 اجباری بر وجود مطلب در همه قسمت‌ها نیست، یک مستد هدف امنیتی که تهدیدها رابیان کرده نیازی به استفاده از OSPs نداد والی آخر، هرچند که هر مستند هدف امنیتی برخی مفروضات را حذف می‌کنند(احتمال کامل نبودن مستند ST به خاطر این حذفیات وجود دارد).

توجه داشته باشید که اگر محصول مورد ارزیابی به طور فیزیکی توزیع شده باشد، بهتر است در خصوص تهدیدهای مرتبط آن ، فرضیات و OSPها به طور مجزا برای حوزه‌های منحصر به فرد از محیط‌های عملیاتی هدف مورد ارزیابی بحث شود.

الف-٦-٢ تهدیدها

این قسمت به برشمردن همه تهدیدهایی می‌پردازد که در محصول مورد ارزیابی، محیط عملیاتی پیرامون یا هردو وجود دارد.

یک تهدید، شامل اجرای عمل مضر و خسارت آوری است که عامل تهدید بر روی سرمایه انجام می‌دهد.

عمل مضر، عملی است که عامل تهدید بر روی یک سرمایه انجام می‌دهد، این عمل تاثیر خود را بر یک یا چند ویژگی از سرمایه که برآن ارزش گذاری شده است اعمال می‌کند.

عاملهای تهدید ممکن است توسط هستارهای مجزا شرح داده شوند، اما در برخی مواقع بهتر است که بر اساس نوع هستارها را گروه بندی کرده و شرح داده شوند.

مثالی از عامل‌های تهدید مانند: نفوذگران، کاربران، پردازش‌های رایانهی و اتفاقات می‌باشند.عامل تهدید می‌تواند از منظر تجربه، منابع، فرصت و انگیزه هم شرح داده شود.

برخی از مثال‌های تهدیدها عبارتند از:

- یک نفوذگر (Hacker) (با در اختیار داشتن تجربه خوب، تجهیزات استاندارد و البته عواید مالی) می‌تواند از راه دور فایل‌های محرمانه را از شبکه هر سازمان کپی کند.
- یک کرم (Worm) به طور بسیار جدی می‌تواند کارایی یک شبکه گسترده WAN را کاهش دهد.
- یک مدیر سامانه ممکن است که حریم خصوصی کاربران را مورد تجاوز قرار دهد.
- کسی که در اینترنت می‌تواند به شنود ارتباطات الکترونیک و محرمانه بپردازد.

الف-٦-٣ سیاست‌ها امنیت سازمانی

این قسمت از تعریف مسئله امنیت، سیاست‌های امنیت سازمانی را نشان می‌دهد که بر محصول مورد ارزیابی، محیط عملیاتی پیرامون آن و ترکیبی از هردو الزام می‌شود.

OSPs: وظایف امنیتی، روالها و راهنماهایی هستند که در حال حاضر یا آینده توسط یک سازمان یا سازمانهای هم نهشت آن ابلاغ و الزام به اجرا در محیط عملیاتی می‌شوند.
سیاست‌های امنیت سازمانی ممکن است برای کنترل محیط عملیاتی محصول مورد ارزیابی توسط یک سازمان، یا مراجع قانون گذار یا تنظیم کننده مقررات تهیه و ابلاغ شود. سیاست‌های امنیتی سازمانی می‌تواند بر محصول مورد ارزیابی یا محیط پیرامون آن اعمال شود.
مثال‌هایی از OSPs:

- همه محصولاتی که در دولت استفاده می‌شود باید، منطبق بر استانداردهای ملی تولید رمز عبور و رمزنگاری باشند.

الف-٦-٤ مفروضات

این قسمت از تعریف مسئله امنیت، مفروضاتی که در محیط عملیاتی پیرامون محصول مورد ارزیابی ایجاد شده است تا ویژگی‌های عملکردی امنیت ارائه شود، را نشان می‌دهد. اگر محصول مورد ارزیابی در محلی واقع گردد که چنین فرضیات و مقرراتی لحاظ نشده باشد، محصول مورد ارزیابی همه ویژگی‌های عملکردی امنیت خودش را ارائه نخواهد داد. مفروضات می‌تواند فیزیکی، پرسنلی و بر حسب ارتباط با محیط پیرامون باشد.
مثال‌هایی از مفروضات:

- مفروضاتی از جنبه‌های فیزیکی محیط عملیاتی پیرامون
- اینگونه فرض می‌شود که محصول مورد ارزیابی در اتاقی که طراحی شده، تا حداقل تجلی امواج الکترومغناطیسی را بروز می‌دهد، استفاده شود.
- اینگونه فرض می‌شود که کنسول‌های مدیریت محصول مورد ارزیابی در شرایط با محدودیت دسترسی جایگذاری می‌شود.
- مفروضاتی از جنبه‌های پرسنل محیط عملیات پیرامون
- اینگونه فرض می‌شود که کاربران محصول مورد ارزیابی به حد کافی برای استفاده از محصول آموزش دیده اند.
- اینگونه فرض می‌شود که کاربران محصول مورد ارزیابی در خصوص اطلاعات طبقه بندی شده در سطح ملی- محرمانه آمادگی دانشی لازم دارند.
- اینگونه فرض می‌شود که کاربران محصول مورد ارزیابی رمزهای عبور خود را در جایی نمی نویسند.
- مفروضات در مورد جنبه ارتباط با محیط عملیاتی پیرامون
- اینگونه فرض می‌شود که یک ایستگاه کاری رایانه شخصی با حداقل فضای‌هارد دیسک 10GB برای اجرای محصول مورد ارزیابی در دسترس است.
- اینگونه فرض می‌شود که محصول مورد ارزیابی تنها محصول منفک از سامانه عامل در حال اجرا در این ایستگاه کاری است.
- اینگونه فرض می‌شود که محصول مورد ارزیابی به هیچ شبکه غیر مطمئنی متصل نیست.
- توجه داشته باشید که در طول فرایند ارزیابی این مفروضات صحیح انگاشته شده و با هیچ حالت دیگری ارزیابی صورت نمی گیرد. به این دلیل، مفروضات به تنهایی می‌توانند محیط عملیاتی پیرامون محصول را

تداعی کنند. مفروضات هرگز بر مبنا رفتار TOE ایجاد نمی شوند، به این علت که ارزیابی به معنای سنجش همه ادعاهایی است که TOE دارد نه در مورد ادعاهایی که بیان می‌کند TOE صحیح هستند.

الف-۷ اهداف امنیت ASE_OBJ

این قسمت شامل خلاصه و چکیده جملاتی است که راه حل‌هایی که برای حل مسئله امنیت تعریف شده اند را بیان می‌کند. وظیفه این قسمت در ۳ بند زیر نشان داده شده است:

- ارائه یک راه حل با زبان طبیعی در یک سطح بالا از انتزاع برای مسئله امنیت
- تقسیم راه حل به دو قسمتی به شکل صحیح به گونه ای که هستارهای مختلف هرکدام بازخوردی از قسمتی از مسئله امنیت را نشان دهد.
- نشان دادن اینکه این قسمت بندی صحیح راه حل جامع و کامل برای مسئله (کل مسئله امنیت را پوشش دهد) باشد.

الف-۷-۱راه حل سطح بالا

قسمت اهداف امنیت شامل مجموعه ای از جملات کوتاه و شفاف بدون هرگونه زیاده گویی در جزئیات است که با هم راه حل سطح بالایی را برای مسئله امنیت مطح می‌کنند. سطح انتزاع اهداف امنیتی بر مبنای قابلیت فهم و دانش مشتری بالقوه TOE می‌باشد بطوری که برای او شفاف باشد. اهداف امنیتی همگی به زبان طبیعی بیان می‌شوند.

الف-۷-۲ تقسیم بندی صحیح راه حل

در مستند هدف امنیتی راه حل امنیتی سطح بالا علاوه بر نشان دادن راه حل، به دو قسمت صحیح تقسیم می‌شود. این قسمتها عبارتند از اهداف امنیتی برای محصول مورد ارزیابی و اهداف امنیتی برای محیط عملیاتی پیرامون محصول. این موضوع نشان دهنده این مطلب است که هر راه حل امنیتی باید هم TOE و هم محیط آن را در نظر بگیرد.

الف-۷-۲-۱ اهداف امنیتی برای TOE

محصول مورد ارزیابی، عملکرد امنیتی را ارائه می‌دهد تا بدین وسیله اطمینان از قسمتی از مسئله امنیت تعریف شده ایجاد شود. به این قسمت اهداف امنیتی برای محصول مورد ارزیابی گفته می‌شود، که شامل مجموعه ای از اهداف است که محصول باید برای حل مسئله امنیتی ارائه کند.

مثالهایی برای اهداف ارزیابی برای محصول مورد ارزیابی:

- محصول مورد ارزیابی باید محرمانگی محتوای همه فایلهایی که بین خودش و سرور انتقال می‌یابد را حفظ کند.
- محصول مورد ارزیابی باید همه کاربران را قبل از اینکه به سرویس انتقال مهیا شده توسط خودش دسترسی بدهد احراز هویت کند.

هدف مورد ارزیابی باید دسترسی کاربران به هر داده را بر مبنای سیاست دسترسی به داده تنظیم کند.

اگر محصول مورد ارزیابی به صورت فیزیکی توزیع شده باشد، بهتر است که قسمت اهداف امنیتی مرتبط با محصول را در مستند ST به زیر قسمت‌هایی تقسیم شود که پوشش کامل را ایجاد کند.

الف-۷-۲-۱۲اهداف امنیتی برای محیط عملیاتی

محیط عملیاتی محصول مورد ارزیابی، مقیاسهای فنی و فرایندی را برای ارائه صحیحی از عملکردهای امنیتی توسط محصول (که در قسمت اهداف امنیتی محصول مورد ارزیابی تعریف شده است) تهیه می‌کند. این قسمت شامل مجموعه ای از جملات است که اهداف اصلی محیط عملیاتی را بیان می‌کند.

مثال‌های از اهداف امنیتی برای محیط عملیاتی:

- محیط عملیاتی باید ایستگاه کاری با سامانه عامل Linux V3.1b برای اجرای TOE بر روی آن ایجاد کند.
- محیط عملیاتی باید این اطمینان را ایجاد کند که همه کاربران انسانی استفاده کننده از محصول قبل از استفاده از آن آموزشهای لازم را دیده اند.
- محیط عملیاتی باید محدودیت‌های فیزیکی دسترسی به محصول را توسط پرسنل مدیریتی و پشتیبان تحت نظارت پرسنل مدیریتی فراهم کند.
- محیط عملیاتی باید اطمینان از محرمانگی ممیزی فایل‌های LOG تولید شده توسط محصول را قبل از ارسال آن به سرور ممیزی فراهم کند.

اگر محیط عملیاتی محصول شامل چندین قسمت، بطوری که هر قسمت با ویژگی‌های خاص خود باشد، بهتر است که قسمت اهداف امنیتی مرتبط با محیط عملیاتی را در مستند ST به زیر قسمت‌هایی تقسیم شود که پوشش کامل را ایجاد کند.

الف-۷-۳ ارتباط بین اهداف امنیتی و مسئله امنیتی تعریف شده

قسمت اهداف امنیتی از مستند هدف امنیتی باید دو قسمت زیر را شامل باشد:

خط سیری که نشانگر برآورده شدن تهدیدها، سیاست‌های امنیت سازمانی و مفروضات توسط اهداف امنیت باشد.

مجموعه ای از دلایل و شواهد که نشان دهد همه تهدیدها، سیاست‌ها سازمانی و مفروضات به شکلی موثر توسط اهداف امنیتی برآورده شده اند.

الف-۷-۳-۱خط سیر رهگیری بین اهداف امنیتی و مسائل امنیتی تعریف شده

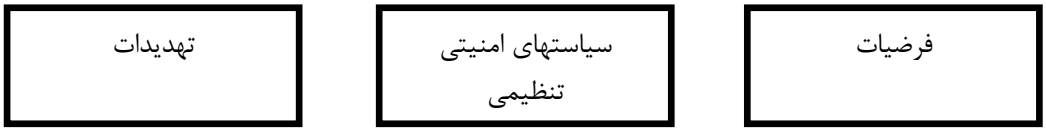
می بایست چگونگی برآورده شدن، تهدیدها، مفروضات و سیاست‌های سازمانی همانگونه که در مسئله امنیتی تعریف شده است توسط اهداف امنیتی بیان شود.

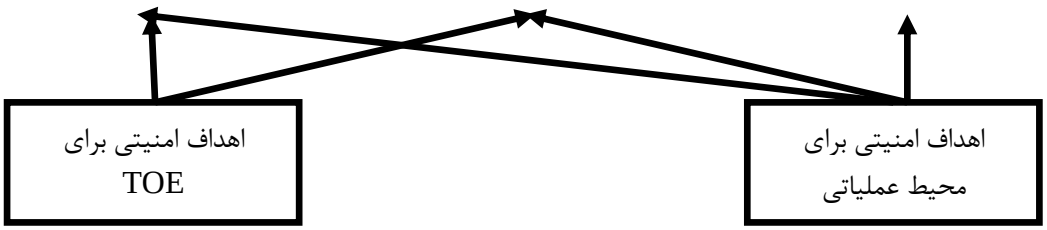
عدم وجود اهداف کاذب: هر هدف امنیتی باید حداقل به یک تهدید، فرض یا سیاست سازمانی منوط باشد.

تطبیق کامل بر مبنای مسئله امنیتی تعریف شده: هر تهدید، سیاست سازمانی یا فرض حد اقل به یک هدف امنیتی رهگیری شود.

رهگیری صحیح: نظر به اینکه فرضیاتی توسط محصول مورد ارزیابی دائما بر محیط ایجاد می‌شوند، اهداف امنیتی برای محصول سیر به عقب به سمت مفروضات را ایجاد نکنند.

قابلیت رهگیری مجاز در قسمت سوم استاندارد ISO/IEC 15408 در شکل زیر نشان داده شده است.





شکل الف-۲-۱خط سیر رهگیری بین اهداف امنیتی و مسائل امنیتی تعریف شده

اهداف امنیتی چند گانه ممکن است به یک تهدید رهگیری شوند، به گونه ای که ترکیبی از این اهداف تهدید را پوشش دهند. بحث مشابه ای در خصوص OSPs و مفروضات هم وجود دارد.

الف-۷-۳-۲ تهیه مجموعه ادله برای رهگیری

اهداف امنیتی نشان دهنده موثر بودن رهگیری هم هستند: همه تهدیدهای داده شده، OSPs و مفروضات در نظر گرفته شده اند (برای مثال: پوشش داده شده، الزام شده و تایید ترتیبی) اگر پیگیری اهداف امنیتی منجر به پوشش آنها شود.

تحلیل اثرات کسب شده از اهداف امنیتی باید نشان دهنده پوشش دادن به تهدیدها، الزامی ساختن OSPs و حمایت از مفروضات شده و نهایتا منجر به اخذ نتایج صحیح در این مورد شود.

در برخی موارد، قسمتی از مسئله امنیت تعریف شده بسیار نزدیک به اهداف امنیتی تعیین شده است و نشان دادن این ارتباط بسیار ساده می‌باشد. برای مثال: تهدید T17: عامل تهدید X اطلاعات محرمانه را در حال انتقال بین A , b می‌خواند، و هدف امنیتی برای محصول OT12: محصول مورد ارزیابی باید اطمینان ایجاد کند که اطلاعات در حال انتقال بین A و B محرمانه نگه داری می‌شود. در این صورت به صورت مستقیم T17 با OT12 مرتبط است.

الف-۷-۳-۳پوشش تهدیدات

پوشش تهدیدات به معنای از بین بردن همه تهدیدات نیست، کاهش به حد کافی تهدیدها و یا تسهیل به اندازه کافی تهدیدها هم می‌تواند مورد نظر باشد.

مثال‌هایی از از بین بردن تهدیدها:

- از بین بردن قابلیت اجرای عمل خسارت باری که عامل تهدید ایجاد می‌کند.
- جابجایی، تغییر حفاظت از سرمایه‌ها به شکلی که عملیات خسارت بار برآنها قابل بکارگیری نباشد.
- حذف عامل تهدید(برای مثال حذف ماشین**هایی که متناوبا باعث نقص در شبکه می‌شوند)**

مثالهایی از تقلیل در تهدیدها:

- محدود ساختن توانایی عامل تهدید در اجرای عملیات خرابکارانه
- محدود ساختن شانس اجرای عملیات خسارت بار توسط عامل تهدید
- کاهش احتمال اجرای عملیات خرابکارانه موفقیت آمیز
- کاهش انگیزه اجرای عملیات خرابکارانه توسط عامل‌های تهدید توسط اعمال ممانعت‌های بازدارنده
- نیاز به کسب تجربه بیشتر و یا منابع بیشتر نسبت به عوامل تهدید

مثالهایی از تسهیل در اثرات تهدید:

- تهیه نسخه‌های پشتیبان به صورت دوره ای از سرمایه‌ها
- تهیه کپی‌های مجزا از یک سرمایه
- بیمه سرمایه‌ها
- کسب اطمینان از اینکه عملیات خرابکارانه قابل شناسایی باشد، آنگاه اقدامات مناسب پس از آن قابل انجام است.

الف-۷-٤ نتیجه قسمت اهداف امنیتی

بر اساس اهداف امنیتی تعیین شده و نمایش داده شده می‌توان این قسمت را تکمیل نمود. اگر همه اهداف امنیت بیان شده مسئله امنیتی تعریف شده را به طور کامل پوشش دهد، مسئله تعریف شده در ASE_SPD حل شده است، همه تهدیدها پوشش داده شده، همه OSPها الزام بر اجرا شده اند و همه مفروضات رعایت شده اند.

الف-۸ مولفه‌های اضافی تعریف شده ASE_ECD

در بسیاری از موارد نیازمندی‌های امنیت در مستند هدف امنیتی بر مبنای قسمت دوم و سوم استاندارد ISO/IEC 15408 تعریف می‌شوند. هرچند، در برخی موارد نیاز به تعریف مولفه ای است که صرحا در قسمت دوم یا سوم استاندارد ISO/IEC 15408 ذکر نشده است. که در چنین مواردی مولفه‌های توسعه یافته باید تعریف شوند.

توجه داشته باشید که این قسمت منحصرا شامل مولفه‌های توسعه یافته می‌باشد نه نیازمندی‌های توسعه یافته(نیازمندی‌هایی که بر اساس مولفه‌های توسعه یافته هستند).

الف-۹ نیازمندی‌های امنیتی ASE_REQ

نیازمندی‌های امنیتی شامل دو گروه از نیازمندی‌ها می‌شود:

الف- نیازمندی‌های عملکردی امنیت (SFRs)، تفسیری از اهداف امنیتی محصول مورد ارزیابی به زبان استاندارد.

ب- نیازمندی‌های ضمانت امنیت (SARs)، توصیفی از چگونگی ضمانت حاصل شده توسط محصول مورد ارزیابی از طریق رعایت SFRs.

این دو گروه از نیازمندی‌ها در ذیل مورد بحث قرار گرفته است.

الف-۹-۱ نیازمندی‌های عملکردی امنیت (SFRS)

مستندSRFs تفسیری از برآورده شدن اهداف امنیت در محصول مورد ارزیابی می‌باشد. این مستندات معمولا با ذکر جزئیات زیاد از سطوح انتزاع هستند، اما باید تفسیر کاملی (اهداف امنیتی باید به طور کامل نشان داده شود) ارائه دهد و از هر راه حل فنی و تکنیکال مستقل(پیاده سازی) باشد، استاندارد ISO/IEC 15408 بنا بر دلایل بسیار زیادی الزام بر تفسیر این نیازمندی‌ها به زبان استاندارد دارد:

- برای ارائه یک توصیف دقیق از هرآنچه قرار است ارزیابی شود. یک هدف امنیتی برای محصول مورد ارزیابی معمولا به شکل زبان طبیعی بیان می‌شود، تفسیر این اهداف به یک زبان استاندارد، الزاما دقت بیشتری در توصیق عملکرد محصول را ایجاد می‌کند.

- اجازه مقایسه بین مستندهای هدف امنیتی ایجاد می‌شود. تفاوت نویسندگان مستندات ارزیابی امنیت ممکن است در استفاده از لغات مختلف در توصیف اهداف امنیت شان باشد،زبان استاندارد الزام به استفاده از لغات یکسان و مفاهیم یکسان می‌دارد ، بنابراین مقایسه آسان را مجاز می‌کند.

تفسیر اهداف امنیتی برای محیط عملیاتی در استاندارد ISO/IEC 15408 الزام نیست، به این علت که محیط عملیاتی مورد ارزیابی قرار نمی گیرد، بنابراین نیازی به ارائه تفسیرهای یکسان نیست.

ممکن است قسمتی از محیط عملیاتی مورد ارزیابی دیگری غیر از ارزیابی محصول قرار گیرد، اما این مسئله خارج از محدوده ارزیابی حال حاضر باشد. برای مثال، یک سامانه عامل اگر محصول مورد ارزیابی باشد، ممکن است نیاز به یک دیواره آتش در محیط عملیاتی پیرامون محصول مورد ارزیابی باشد. تحت یک عملیات ارزیابی دیگر می‌توان در ادامه دیواره آتش را ارزیابی کرد، ولی این ارزیابی هیچ ارتباطی با ارزیابی سامانه عامل نخواهد داشت.

الف-۹-۱-۱چگونه ISO/IEC 15408 از این تفسیر حمایت می‌کند

استاندارد ISO/IEC 15408 از تفسیر اهداف امنیتی به زبان استاندارد به دو شکل زیر پشتیبانی می‌کند:

الف- از طریق تهیه یک زبان خلاصه از پیش تعریف شده، که دقیقا برای توصیف دقیق ارزیابی طراحی شده باشد. این زبان از مجموعه از مولفه‌ها تشکیل شده است که در قسمت دوم استاندارد ISO/IEC 15408 معرفی شده اند. استفاده از این زبان بعنوان یک ساختار خوش تعریف برای تفسیر اهداف امنیتی محصول که نیازمندی‌های عملکردی امنیت را الزام دارد، در همین قسمت (قسمت ۸-۳) از استاندارد بیان شده است.

ب- با ارئه مجموعه عملیات، مکانیسم‌هایی که نویسنده مستند هدف امنیتی را مجاز به تغییر نیازمندی‌های عملکردی امنیت می‌دارد تا تفسیر دقیق تری از اهداف امنیتی برای محصول ایجاد شود. این قسمت از استاندارد ISO/IEC 15408 چهار عملیات، تخصیص، انتخاب، تکرار و پایش را معرفی کرده است(قسمت۸-۱).

ج) از طریق ارائه وابستگی‌ها، مکانیسمی برای پشتیبانی از تفسیر کامل مستند نیازمندی‌های عملکردی امنیت. این زبان در قسمت دوم استاندارد ISO/IEC 15408 این گونه است که هر نیازمندی عملکردی امنیت می‌تواند به یک نیازمندی دیگر وابسته باشد. بدین معنا که هر مستند هدف امنیتی که از یک نیازمندی از این نوع استفاده کند باید همه وابستگی‌های آن را نیز ذکر کند. این مسئله نوشتن مستند هدف امنیتی که همه نیازمندی‌های الزامی را پوشش دهد و از سوی دیگر جامعیت را در مستند حفظ کند بسیار دشوار می‌کند. وابستگی‌ها در قسمت ۸-۲ توضیح داده شده است.

الف-۹-۱ ارتباط بین SFRs و اهداف امنیتی

مستند هدف امنیتی همچنین شامل بیانی از نیازمندی‌های امنیتی است که از طریق دو قسمت زیر نشان می‌دهد:

الف- رهگیری اینکه چه نیازمندی عملکردی هدف امنیتی را برآورده می‌سازد.

ب) مجموعه ای از دلایل که نشان دهد همه اهداف امنیتی برای محصول به طور موثری توسط نیازمندی‌های عملکردی امنیت برآورده شده اند.

الف-۹-۱-۲-۱رهگیری بین مستند نیازمندی‌های عملکرد امنیت و اهداف امنیت برای محصول

دنباله گیری نشان می‌دهد که چگونه مستند نیازمندی‌های عملکردی بازگشت به اهداف امنیتی برای محصول می‌کند، در ادامه بیان شده است:

الف-جعلی نبودن نیازمندی‌های عملکردی امنیت، هر مستند عملکردی امنیت باید بازگشت به حداقل یک هدف امنیت داشته باشد.

ب-پوشش کامل اهداف امنیتی برای محصول، هر هدف امنیتی برای محصول مورد ارزیابی باید به حداقل یک نیازمندی عملکردی منوط باشد.

چندین نیازمندی‌های عملکردی ممکن است به یک هدف امنیتی برای محصول مورد ارزیابی اشاره کند که این ادغام نیازمندی‌های امنیتی باید هدف امنیتی محصول را برآورده سازد.

الف-۹-۱-۲-۲ تهیه مجموعه ادله رهگیری

مجموعه دلایل نیازمندی‌های امنیتی باید نشان دهد که دنباله گیری آن به شکل موثر است: اگر همه نیازمندی‌های عملکردی ارجاع شده به یک هدف امنیتی خاص برای محصول مورد ارزیابی رضایت قسمت باشد، به گونه ای که هدف امنیتی برای محصول برآورده شده باشد.

نمایش ادله باید تحلیل اثر رضایت مندی از نیازهای عملکردی امنیت مرتبط که منجر به حصول هدف امنیتی برای محصول شده است را نشان دهد، و نتیجتا باعث کسب اطمینان از صحت و درستی مورد شود.

در این موارد هرگاه نیازهای عملکردی امنیت شباهت بسیار زیادی به اهداف امنیت برای محصول داشته باشند نشان دادن این ارتباط بسیار ساده خواهد بود.

الف-۹-۲ نیازمندی‌های ضمانت امنیتی

نیازمندی‌های ضمانت امنیت به توصیف چگونگی ارزیابی محصول می‌پردازد. برای انجام این توصیف از یک زبان استاندارد به دو دلیل زیر استفاده می‌شود.

- برای ارائه یک توصیف دقیق از هرآنچه قرار است ارزیابی شود. از یک زبان استاندارد که موجب دقت در توصیف فارق از هر گونه ابهام بیانجامد استفاده شود.
- اجازه مقایسه بین مستندهای هدف امنیتی ایجاد می‌شود. تفاوت نویسندگان مستندات ارزیابی امنیت ممکن است در استفاده از لغات مختلف در توصیف اهداف امنیت شان باشد،زبان استاندارد الزام به استفاده از لغات یکسان و مفاهیم یکسان می‌دارد ، بنابراین مقایسه آسان را مجاز می‌کند.

این زبان استاندارد در قسمت سوم از استاندارد ISO/IEC 15408 تحت قالب مجموعه ای از مولفه‌ها تعریف شده است. استفاده از این زبان اجباری است هرچند که برخی استثناءها وجود دارند. استاندارد ISO/IEC 15408 استفاده از این زبان را به دو شکل بیان می‌دارد:

الف- با ارئه مجموعه عملیات، مکانیسم‌هایی که نویسنده مستند هدف امنیتی را مجاز به تغییر نیازمندی‌های ضمانت امنیت می‌دارد تا تفسیر دقیق تری از اهداف امنیتی برای محصول ایجاد شود. این قسمت از استاندارد ISO/IEC 15408 چهار عملیات، تخصیص، انتخاب، تکرار و پایش را معرفی کرده است(قسمت۸-۱).

ج) از طریق ارائه وابستگی‌ها، مکانیسمی برای پشتیبانی از تفسیر کامل مستند نیازمندی‌های ضمانت امنیت. این زبان در قسمت سوم استاندارد ISO/IEC 15408 این گونه است که هر نیازمندی ضمانت امنیت می‌تواند به یک نیازمندی دیگر وابسته باشد. بدین معنا که هر مستند هدف امنیتی که از یک نیازمندی از این نوع استفاده کند

باید همه وابستگی‌های آن را نیز ذکر کند. این مسئله نوشتن مستند هدف امنیتی که همه نیازمندی‌های الزامی را پوشش دهد و از سوی دیگر جامعیت را در مستند حفظ کند بسیار دشوار می‌کند. وابستگی‌ها در قسمت ۸-۲ توضیح داده شده است.

الف-۹-۳ نیازمندهای ضمانت امنیت و ادله نیازمندی‌های امنیت

مستند هدف امنیتی شامل مجموعه ای از نیازهای امنیتی است که نشان می‌دهد چرا یک مجموعه از نیازمندی‌های ضمانت تخصیص داده شده است. هدف این توصیف ایجاد توانایی برای خوانندگان برای درک دلایل اینکه چرا یک مجموعه انتخاب شده است، می‌باشد.

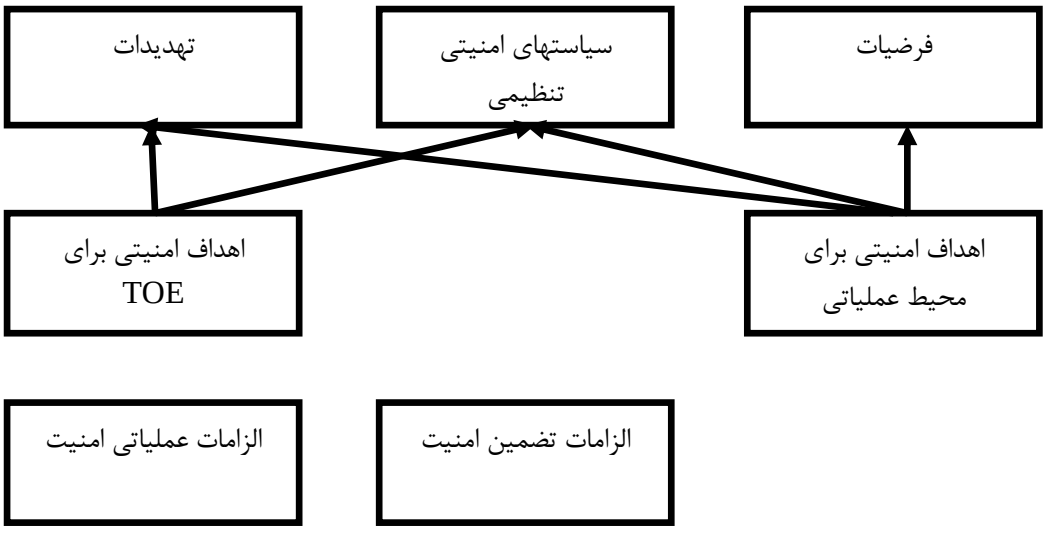
یک مثال از این تناقص این است که اگرف یک مسئله امنیتی تعریف شده، تهدیدی را نشان دهد که عامل تهدید بسیار توانمند باشد، و یک تحلیل حفره ضعیف یا نامناسب انتخاب شود این مسئله SAR مشخص می‌شود.

الف-۹-٤ نتایج الزامات امنیت

در قسمت تعریف نیازمندی امنیت از مستند هدف امنیتی ، مسئله امنیتی تعریف شد که شامل تهدیدها، سیاست‌های سازمانی و مفروضات بوده است، در قسمت اهداف امنیتی از مستند هدف امنیتی راه حل ارائه می‌شود که شامل دو زیر قسمت اصلی است:

- اهداف امنیتی برای هدف امنیتی
- اهداف امنیتی برای محیط عملیاتی پیرامون هدف مورد ارزیابی

بعلاوه، اهداف امنیتی نشان میدهد که اگر همه اهداف امنیتی برآورده شوند، مسئله امنیتی تعریف شده حل شده است، همه تهدیدها پوشش داده شده، همه سیاست‌های امنیتی سازمان الزام و ابلاغ شده و همه مفروضات حمایت شده اند.



شکل الف-۳ - نمایش ارتباط بین تعریف مسئله امنیتی، اهداف امنیتی و نیازمندی‌های امنیتی

در قسمت نیازمندی‌های امنیتی در مستند هدف امنیتی ، اهداف امنیتی برای TOE، تحت قالب نیازمندی‌های عملکردی امنیت تفسیر شده و یک شمایی از نیازمندی‌های امنیت تهیه می‌شود که نشان دهنده این مسئله

است که همه نیازمندی‌های عملکردی امنیت رضایت قسمت هستند و همه اهداف امنیتی برای محصول برآورده شده است.

بعلاوه مجموعه ای از نیازمندی‌های ضمانت تهیه شده است که نشان می‌دهد چگونه یک محصول ارزیابی شود، به همراه توضیحاتی از اینکه چگونه این مجموعه از نیازمندی‌های ضمانت امنیت انتخاب شده است.

همه این جملات می‌تواند اینگونه ترکیب شود که: همه نیازمندی‌های کارکردی امنیت و نیازمندی‌های ضمانت امنیت رضایت قسمت بوده اند و همه اهداف امنیتی برای محیط عملیاتی پیرامون برآورده شده اند. و در نتیجه ضمانتی از اینکه مسئله امنیتی تعریف شده است در ASE_SPD حل شده باشد، ایجاد شود. همه تهدیدها پوشش داده شده باشد، همه سیاست‌های امنیت سازمان ابلاغ و الزام شده باشد و همه مفروضات حمیات ده باشد. این مسئله در شکل ۷ نشان داده شده است.

میزان ضمانتی که کسب می‌شود توسط نیازمندی‌های ضمانت امنیت تعریف می‌شود، به گونه ای که میزان ضمانت مکفی بر اساس توضیحاتی که برای الزامات ضمانت امنیت و انتخاب آنها ارائه شده است، تعیین می‌گردد.

الف-۱۰ خلاصه توضیحاتی در مورد محصول مورد ارزیابی

هدف این قسمت تهیه توضیحاتی از چگونگی برآورده سازی نیازمندی‌های کارکردی امنیت محصول توسط محصول مورد ارزیابی به مشتریان بالقوه می‌باشد. این قسمت توضیح خلاصه ای از مکانیسم‌های فنی بکار رفته در محصول مورد ارزیابی برای دست یافتن به این هدف را ارائه می‌کند. سطح جزئیات این تشرح باید به اندازه ای کافی باشد که مشتریان بالقوه درک جامعی از پیاده سازی محصول مورد ارزیابی به دست بیاورند.

برای نمونه اگر محصول مورد ارزیابی یک Internet PC باشد و مستند نیازمندی‌های عملکردی آن شامل FIA_UAU.1، باشد برای انجام احراز هویت، این قسمت از مستند TOE باید نشان دهد که چگونه احراز هویت انجام می‌شود، از طریق یک پسورد، Token و یا غیره. اطلاعات بیشتر استاندارد به کار رفته برای برآروده ساختن نیازمندی عملکردی توسط محصول مورد ارزیابی یا توضیحات بیشتر ممکن است ارائه شود.

الف-۱۱ سئوالاتی که ممکن است توسط مستند هدف امنیتی پاسخ داده شود

پس از ارزیابی، مستند هدف امنیتی بیان می‌دارد که «چه چیزی ارزیابی شده است». در این وظیفه، مستند هدف امنیتی بعنوان یک توافق بین توسعه دهنده و بازاریاب و مشتریان بالقوه محصول مورد ارزیابی عمل می‌کند. مستند هدف امنیتی می‌تواند نتیجتا سئوالات زیر را پاسخ دهد:

الف-چگونه یک ST/TOE که نیازمند آن هستیم را از مجموعه همه TOE/STهای موجود انتخاب کنیم؟ این سئوال در قسمت مرور ب TOE پاسخ داده می‌شود، که خلاصه ای از محصول مورد ارزیابی داده می‌شود.

ب)آیا محصول مورد ارزیابی با ساختار فنآوری سازمان ما مناسب است؟ این سئوال در قسمت مرور بر TOE پاسخ داده می‌شود، به گونه ای که مهمترین سخت افزارها و نرم افزارها و میان افزارهایی که برای اجرای TOE لازم هستند را بیان می‌کند.

پ)آیا محصول مورد ارزیابی با محیط عملیاتی موجود سازمان ما سازگار است؟ این سئوال در قسمت اهداف امنیتی برای محیط عملیاتی پیرامونی پاسخ داده می‌شود، به گونه ای که همه محدودیت‌هایی که محصول در محل اجرا با آن مواجه است را بیان می‌کند.

ت)محصول مورد ارزیابی چه کاری انجام می‌دهد؟ (خوانندگان علاقه مند) این سئوال در قسمت مرور بر TOE پاسخ داده می‌شود، اینگونه که خلاصه ای از رفتارTOE بیان می‌شود.
ث)محصول مورد ارزیابی چه کاری انجام می‌دهد؟ (مشتریان بالقوه) این سئوال در قسمت توصیف خلاصه TOE پاسخ داده می‌شود، اینگونه که خلاصه ای از رفتارTOE بیان می‌شود.
ج)محصول مورد ارزیابی چه کاری انجام می‌دهد؟ (خبرگان) این سئوال در قسمت نیازمندی‌های عملکردی امنیت در سطح انتزاعی از توضیحات فنی بیان می‌شود، و همچنین قسمت توصیف خلاصه از محصول مرود ارزیابی جزئیات بیشتری را ارائه می‌دهد.
چ)آیا محصول مورد ارزیابی مسئله امنیتی که توسط دولت/سازمان تعریف شده است را پوشش می‌دهد؟ اگر دولت یا سازمان رخ‌نمون محافظتی یا بسته‌هایی را بعنوان راه حل تعریف کرده باشد، پاسخ این سئوال می‌تواند در قسمت ادعای تطبیق از مستند هدف امنیتی جستجو شود، که فهرستی از بسته‌ها و رخ‌نمون‌های محافظتی که مستند هدف امنیتی از آنها استفاده کرده است را نشان می‌دهد.
ح)آیا محصول مسئله امنیتی تعریف شده را پوشش می‌دهد؟ (خبرگان) چه تهدیدهایی توسط محصول مورد ارزیابی پوشش داده شده اند؟ چه سیاست‌های امنیت سازمانی الزام بر اجرا یافته اند؟ چه مفروضات در خصوص محیط عملیاتی در نظر گرفته شده است؟ همه این سئوالات در قسمت تعریف مسئله امنیتی پاسخ داده می‌شود.
خ)چه میزان اطمینان به محصول مورد ارزیابی می‌توان داشت؟ پاسخ این سئوال در مستند نیازمندی‌های ضمانت امنیت در قسمت الزامات امنیتی یافت، اینکه کدام سطح ضمانت برای ارزیابی محصول به کار رفته است، و در نتیجه به همان اندازه اطمینان از صحت محصول ایجاد می‌شود.

الف-۱۲ مستندات هدف امنیتی با حداقل ضمانت

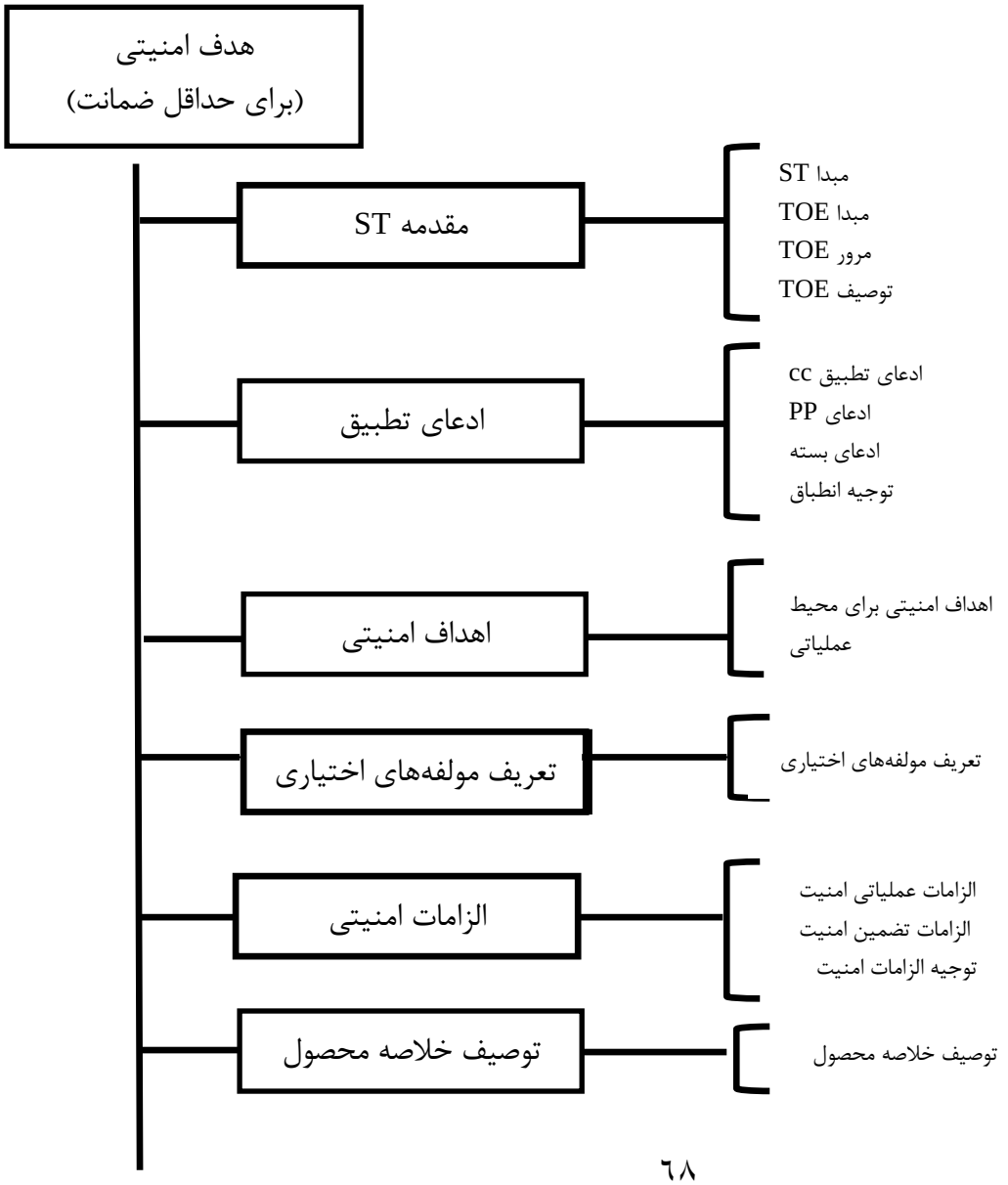
طراحی یک مستند هدف امنیتی مسئله ای کم ارزش نیست و ممکن است طراحی یک مستند برای دست یافتن به حداقل میزان ضمانت قسمت بسیار بزرگی از تلاشهای توسعه دهنده یا ارزیاب برای اجرای عمل ارزیابی در کل باشد. به این دلیل، ممکن است نیاز به طراحی مستند هدف امنیتی با حداقل ضمانت باشیم.
استاندارد ISO/IEC 15408 اجازه طراحی مستند هدف امنیتی با حداقل سطح ضمانت را برای اخذ سطح ا یعنی EAL 1 مجاز می‌دارد ولی برای سطوح ۲ به بالاتر مجاز نیست. یک مستند با حداقل سطح ضمانت ممکن است ادعای تطبیق با مستند رخ‌نمون محافظتی با حداقل ضمانت داشته باشد (پیوست ب). به طور معمول هر مستند هدف امنیتی (حتی با وجود کامل بودن محتوی) ممکن است فقط ادعای تطبیق با حداقل سطح ضمانت مطرح شده در یک رخ‌نمون محافظتی را بیان کند.
یک مستند هدف امنیتی با حداقل سطح ضمانت محتوی قابل مقایسه حداقلی را ارائه می‌کند:

- نیاز به تعریف مسئله امنیت وجود ندارد
- نیاز به توصیف اهداف امنیت برای محصول وجو ندارد، ولی همچنان اهداف امنیتی برای محیط پیرامون محصول باید مطرح شود.
- نیازی به شرح شمای اهداف امنیت همانطور که مسئله امنیت تعریف نشده، نخواهد بود.
- شمای نیازمندی‌های امنیتی فقط به جهت برآورده سازی وابستگی‌ها نیاز هستند و همانطور که اهداف امنیتی برای محصول مورد ارزیابی تعریف نشده است این قسمت هم نیاز نیست.

همه قسمت‌های باقیمانده در ذیل آمده است:

- مراجع محصول و مستند هدف امنیتی
- ادعای تطبیق
- توصیف رویه مختلف
- مرور بر محصول مورد ارزیابی
- توصیف محصول مورد ارزیابی
- خلاصه توصیف محصول مورد ارزیابی
- اهداف امنیتی برای محیط عملیاتی
- نیازمندی‌های عملکردی امنیت و نیازهای ضمانت امنیت (شامل مولفه‌های اضافی تعریف شده) و شمای نیازمندی‌های امنیت (فقط اگر وابستگی برآورده نشده باشد)

شکل الف-۴ محتوای کاهش یافته از مستند هدف امنیتی با حداقل ضمانت بیان شده است.



شکل الف-٤ محتوای کاهش یافته از مستند هدف امنیتی با حداقل ضمانت

الف-۱۳ ارجاع به دیگر استانداردها در یک مستند هدف امنیتی

در برخی موارد، نویسنده مستند هدف امنیتی ممکن است از استانداردهای خارجی بعنوان منبع استفاده کند، مانند یک استاندارد یا پروتکل خاص رمزنگاری. استاندارد ISO/IEC 15408 در سه شکل زیر این مسئله را مجاز می‌دارد:

الف-بعنوان یک سیاست امنیت ابلاغی سازمانی

برای مثال یک استاندارد ملی وجود داشته باشد که چگونگی انتخاب گذرواژه در آن بیان شده باشد، ممکن است این استاندارد تحت قالب سیاست امنیت سازمانی به درون مستندهدف امنیتی وارد شود و یک هدف برای محیط ایجاد کند(برای مثال اگر کاربران محصول مورد ارزیابی نیاز به انتخاب گذرواژه منطبق برآن شرایط داشته باشند). یا منجر به اهداف امنیتی برای محصول مورد ارزیابی گردد که در این صورت نیازمندی‌های عملکردی امنیت مناسب تهیه می‌شود(همانند کلاس FIA)اگر محصول به تولید گذرواژه بپردازد. در هر دو حالت شمای نیازهای توسعه دهنده اهداف امنیتی برای محصول را قابل پذیرش می‌سازد و نیازهای عملکردی امنیت به تناسب سیاست‌های امنیتی تبیین می‌شوند. از نظر ارزیاب اگر این مسئله قابل پذیرش باشد باید آزمایش شود، (ممکن است تصمیم به مطالعه استاندارد استفاده شده بگیرد) اگر سیاست امنیت سازمانی توسط نیازمندی‌های عملکردی امنیت پیاده سازی شده باشد که در ذیل توضیح داده شده است.

ب-همانند یک استاندارد فنی (برای مثال استانداردهای رمز نگاری) در عملیات پایش نیاز عملکردی به کار گرفته شود.

در این مورد تطابق با استاندارد قسمتی از تکامل نیازهای عملکردی امنیت توسط محصول مورد ارزیابی است و تمامیت استاندارد بعنوان قسمتی از نیازهای عملکردی امنیت در نظر گرفته شود. تطبیق به طور سلسه مراتبی پ)همانند دیگر تطابق‌ها در نیازمندی‌های عملکردی امنیت می‌باشد، در طول ADV، توسعه و ATE، آزمون و تحلیل، طراحی و تحلیل‌ها و آزمون‌ها که نیازمندی‌های عملکردی امنیت به طور کامل در محصول پیاده سازی شده است.و اگر مراجع به یک قسمت قابل اطمینان از یک استاندارد اشاره داشته باشد، آن قسمت باید بصورت غیر مبهم در عملیات پایش نیازمندی‌های عملکردی امنیت بیان شود.

بعنوان یک استاندارد فنی (برای مثال یک استاندارد رمزنگاری) که در قسمت توصیف خلاصه محصول مورد ارزیابی به آن اشاره شود.

توصیف خلاصه محصول مورد ارزیابی بعنوان قسمتی که توضیح دهد چگونه نیازهای عملکردی کسب شده اند، مورد نظر می‌باشد، و استفاده محدود برای پیاده سازی محدود نیازمندی‌های مشابه نیازمندی‌های عملکردی امنیت نست یا مستندات قابل تحویل برای ADV، توسعه. بنابراین ارزیاب ممکن است مغایرت مراجع TSS و استانداردهای فنی را تشخیص دهد و این مسئله اثری در ADV، مستندات توسعه نداشته باشد. اما هیچ فعالیت عادی برای آزمون تناسب و تکمیل بودن این استاندراد وجود ندارد.

پیوست ب

(اطلاعاتی)
شرح مستند رخ‌نمون محافظتی

ب-۱ هدف و ساختار این پیوست

هدف این پیوست شرح مفاهیم مستند رخ‌نمون محافظتی است. این پیوست ضوابط مربوط به کلاس APE را معرفی نمی کند، و این ضوابط در قسمت سوم استاندارد ISO/IEC 15408 مطرح شده است.

به دلیل آنکه مستندات رخ‌نمون محافظتی و هدف امنیتی هم پوشانی زیادی دارند، در این پیوست بیشتر به شرح تفاوت‌های بین این مستندات می‌پردازیم. محتوای مفاد این مستند در پیوست الف قابل شناسایی است.

این پیوست در چهار محور اساسی زیر بحث می‌کند:

الف-مستند رخ‌نمون محافظتی شامل چه‌ها (What) باید(Must) باشد. الزامات اجباری که در محتوای رخ‌نمون محافظتی باید قرار گیرد، روابط بین این قسمت‌ها با ذکر مثال‌هایی بیان می‌شود.

ب-چگونه (HOW) باید(Should) از مستند رخ‌نمون محافظتی استفاده کرد.

پ)مستندهای رخ‌نمون محافظتی با حداقل سطح ضمانت می‌کنند. مستندهای رخ‌نمون محافظتی که محتوی کاهش یافته ای دارند.

ت)اظهار ادعا به شکل استاندارد. این مسئله که چگونه یک نویسنده مستند رخ‌نمون محافظتی می‌تواند ویژگی‌های خاصی که محصول (TOE) می‌تواند بعنوان استاندارد ویژه از آن اخذ کند، را بیان کند.

ب-۲ مندرجات اجباری در مستند رخ‌نمون محافظتی

شکل ب-۱ همه مندرجات الزامی که مستند رخ‌نمون محافظتی منطبق بر مفاد قسمت سوم استاندارد ISO/IEC 15408 باید داشته باشد را به تصویر کشیده است. این شکل می‌تواند یک نقشه اجمالی از ساختار مستند رخ‌نمون محافظتی در نظر گرفته شود هرچند که هر ساختار دیگر (ضمن رعایت الزامات قسمت سوم ISO/IEC 15408) مجاز می‌باشند. برای مثال، اگر الزامات امنیتی بسیار زیادی وجود داشته باشد، می‌توان قسمتی از این الزامات را در یک پیوست در مستند رخ‌نمون محافظتی قرار داد به جای اینکه همه این حجم انبوه مطالب را در قسمت الزامات امنیتی مستند رخ‌نمون محافظتی قرار داده شود. قسمت‌های مجزای یک مستند رخ‌نمون محافظتی و محتوی آنها به شکل خلاصه در زیر مطرح شده اند. یک مستند رخ‌نمون محافظتی به طور معمول شامل:

الف-مقدمه، شامل خلاصه کوتاه و توصیفی از نوع محصول است.

ب- ادعای تطبیق، قسمت‌هایی از PP که منطبق بر هر PP (ها) یا بسته (ها) هستند در این قسمت نشان داده می‌شود.

ج) تعریف مسئله امنیت، نشان دهنده تهدیدها، OSPs، و همه مفروضات امنیتی را نشان می‌دهد.

د)اهداف امنیتی، نشان دهنده این است که چگونه برآورده شدن یک مسئله امنیتی توسط تقسیم آن به شکل اهداف امنیتی برای محصول و محیط عملیاتی پیرامون محصول انجام می‌شود.

ه)تعریف مولفه‌های اضافی، هر گاه مولفه جدید (علاوه برآنچه در قسمت دوم و سوم ISO/IEC 15408 بیان شده است) تعریف شود، این مولفه‌های جدید باید تحت قالب مولفه‌های عملکردی امنیت و مولفه‌های ضمانتی امنیت اضافی تعریف شوند.

و) الزامات امنیتی، درواقع تفسیری از یک هدف امنیتی برای محصول در قالب یک زبان استاندارد است. این زبان استاندارد درون مستندات SFRs و SARs است.

مستند رخ‌نمون محافظتی با حداقل سطح ضمانت با مندرجات کاهش یافته هم وجود دارد که در انتهای این پیوست توضیح داده می‌شود، بطور کلی این پیوست یک مستند رخ‌نمون محافظتی کامل و جامع را در نظر می‌گیرد.

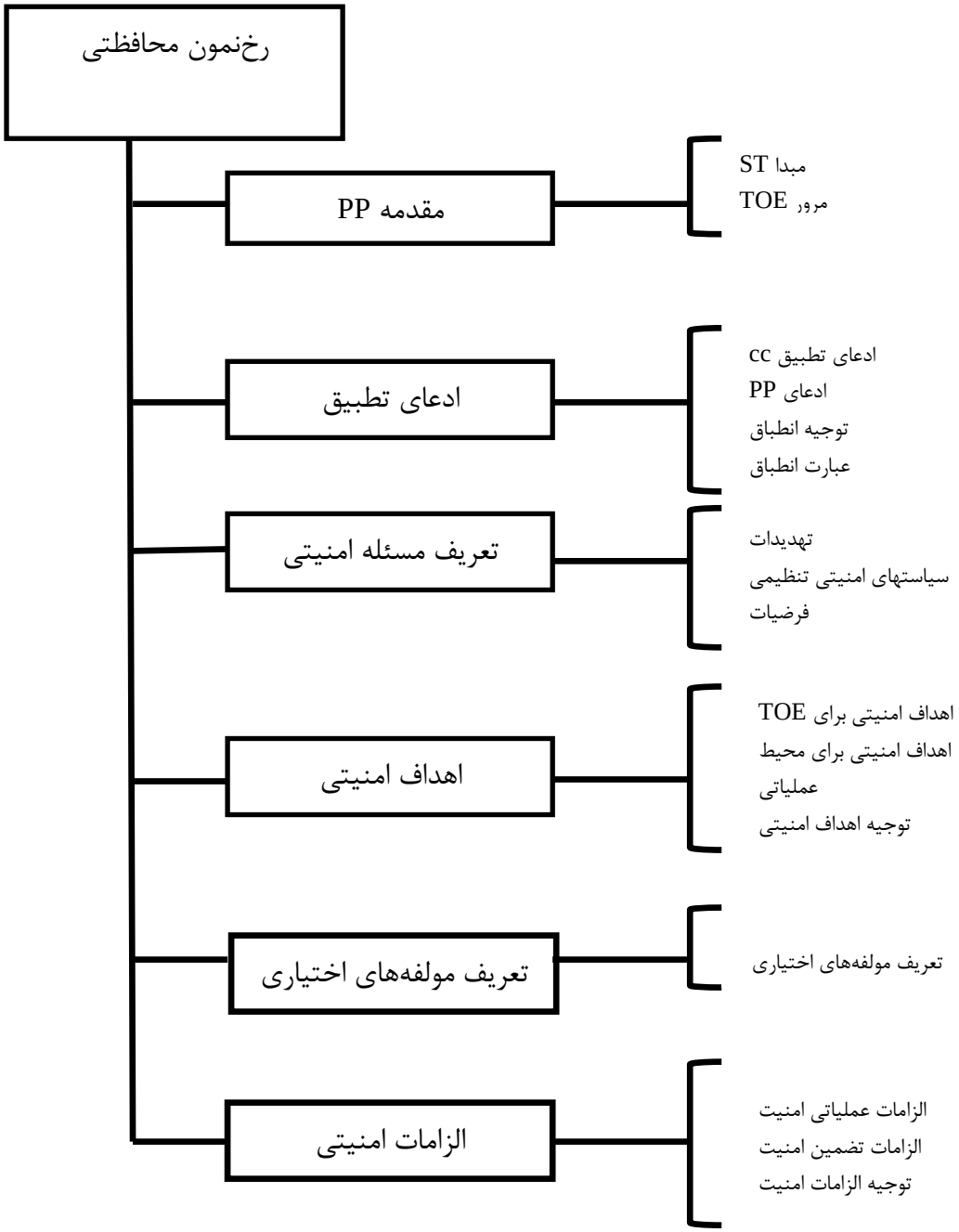
ب-۳ استفاده از مستند رخ‌نمون محافظتی

ب-۳-۱ چگونه باید از یک مستند رخ‌نمون محافظتی استفاده کرد

هر مستند رخ‌نمون محافظتی به صورت عمومی به گونه ای است که، مجموعه ای از کاربران، مراجع قانونی، گروه توسعه دهندگان وتولید کنندگان مجموعه ای از نیازهای امنیتی مشترک خود را تعریف می‌کنند. یک رخ‌نمون محافظتی به مشتریان بعنوان ابزاری برای ارجاع به این مجموعه نیازمندی‌ها و سهولت ارزیابی‌های آتی در قبال این نیازمندی‌ها کمک می‌کند.

هر مستند رخ‌نمون محافظتی به صورت عموم به روشهای زیر استفاده می‌شود:

- قسمتی از نیازمندی توصیف شده برای یک مشتری خاص یا گروهی از مشتریان، به گونه ای که قصد تهیه نوعی خاص از تجهیزات فنآوری را داشته باشند به شرط آنکه نیازمندی‌های مندرج در رخ‌نمون محافظتی را برآورده ساخته باشد.
- قسمتی از فرم‌های قانونی هر مرجع قانون گذاری به گونه ای که فقط نوع خاص از تجیهزات فنآوری را در صورت برآورده ساختن الزامات رخ‌نمون محافظتی مجاز اعلام کند.
- تعیین خط مشی برای گروه توسعه دهندگان و تولید کنندگان محصولات فنآوری به گونه ای که همه محصولات تولید شده از نوع خاص مطرح شده در رخ‌نمون محافظتی باید حد و مرز اعلام شده آن را رعایت کند.
- شرح ای از یک محصول منفرد، برخلاف مستند هدف امنیتی ، مستند رخ‌نمون محافظتی برای شرح شرایط اطمینان از رده ای از محصولات فنآوری طراحی شده است، و برای یک محصول منفرد نیست. هرگاه شرح یک محصول منفرد مورد نیاز باشد استفاده از یک مستند هدف امنیتی بهتر است.



شکل ب-۱ - محتوای رخ‌نمون محافظتی

ب-٤-١ مستندات مرجع PP[1]

یک مستند رخ‌نمون محافظتی باید به صورت شفاف مراجعی را معرفی کند که ویژه آن مستند است. بصورت عمومی باید، عنوان، نسخه، نویسنده و تاریخ نشر مستندات عنوان شود. بعنوان مثال:

"Atlantean Navy CablePhone Encryptor PP,version 2b, Atlantean Navy Procurement Office, April 7, 2003".

1- PP Reference

مراجع باید منحصر به فرد باشند به این دلیل که امکان تفکیک مستندات رخنمون محافظتی مختلف و نسخه‌های مختلف از یک مستند رخنمون محافظتی از هم وجود داشته باشد.

ب-۲-٤ مرور بر TOE

این قسمت با هدف کمک به مشتریان بالقوه ای است که از فهرست محصولات ارزیابی شده در جستجوی محصولی هستند که نیاز آنها را برآورده سازد و از سوی دیگر با تجهیزات مورد نظر مشتریان از نظر سخت افزاری و نرم افزاری و میان افزاری مطابقت دارد.

این قسمت با هدف کمک به توسعه دهندگانی که از مستند پروفال محافظتی برای طراحی محصولات مورد ارزیابی و یا برای تطبیق محصولات موجود از آن استفاده می‌کنند، نیز طراحی شده است. به طور معمول این قسمت شامل چندین پاراگراف است.

به همین دلیل، این قسمت توصیف خلاصه ای از موارد استفاده محصول و مهمترین خصیصه‌های امنیتی، نوع محصول و نیازمندی‌های تجهیزاتی (سخت افزار، نرم افزار، لخت افزار) به جز محصول مورد ارزیابی (NON - TOE)آن را توصیف می‌کند.

ب-٤-۲-۱ موارد استفاده و مهمترین خصیصه‌های محصول[1]

در این قسمت، ایده کلی از آن چه توانایی محصول از نظر امنیت است، و آن استفاده ای که در حوزه امنیت از محصول می‌شود ارائه می‌گردد. این قسمت برای مشتریان بالقوه نوشته می‌شود، توصیف خصیصه‌های مهم امنیتی و نوع استفاده آن در عملیات کسب و کار و تجارت به زبانی که قابل فهم برای مشتری باشد انجام می‌شود.

بعنوان مثال: .”The Atlantean Navy CablePhone Encryptor“ یک ابزار رمزنگار است که امکان ایجاد ارتباط محرمانه بین کشتی‌ها را در سامانه مخابراتی The Atlantean Navy CablePhone محیا می‌کند. برای دست یافتن به این هدف ۳۲ کاربر مختلف به طور همزمان قابلیت استفاده از آن را دارند و حداقل 100Mbps سرعت در انتقال داده دارد. این محصول قابلیت ارتباط دو طرفه بین کشتی‌ها و همچنین پخش سراسر در شبکه را دارا است.

ب-٤-۲-۲ نوع TOE [2]

در قسمت مرور بر TOE باید بصورت عمومی نوع TOE مشخص شود، مانند اینکه: دیوار آتش، VPN-Firewall، کارت هوشمند، مودم رمزنگار، اینترانت، وب سرور، پایگاه داده، شبکه محلی و سراسری با پایگاه داده و وب سرور و غیره.

1- Usage and Major Security Features of a TOE
2-TOE Type

ب -۴-۲-۳ نیازمندی‌های سخت افزاری/نرم افزاری/لخت افزاری غیر از هدف مورد ارزیابی[1]

هرچند که بسیار از محصولات مورد ارزیابی به هیچ محصول فنآوری دیگری تکیه ندارند، ولی بسیاری از محصولات مورد ارزیابی (خصوصا نرم افزارها) به صورت اضافی به برخی از تجهیزات وابسته هستند. بعبارت دیگر، در قسمت مرور TOE باید این نوع وابستگی‌ها بیان شود.

در یک مستند رخنمون محافظتی، محصول خاص شرح داده نمی‌شود، در بسیاری از موارد تنها ایده‌های کلی در مورد تجهیزات فنآوری (سخت افزاری/نرم افزاری/لخت افزاری)ارائه می‌شود. بیان نیازمندی‌های خاص برای مشتریان خاص به گونه ای که نسبت به بسترهای زیر ساختی مورد نیاز خود آشنا باشند، اطلاعاتی بیشتری می‌توان ارائه داد.

برای مثال:

- هیچ، برای محصولات مورد ارزیابی غیر وابسته به محیط
- یک سامانه عامل Yaiza نسخه 3.0 بر روی یک رایانه رو میزی.
- یک مدار مجتمع CleverCard SB2067
- یک مدار مجتمع CleverCard SB2067 به همراه سامانه عامل کارت هوشمند QuickOS V2.0

ب-۵ ادعای تطبیق (APE_ISO/IEC 15408L) [2]

این قسمت مستند رخنمون محافظتی چگونگی تطبیق مستند بادیگر مستندات رخنمون محافظتی و بسته‌ها را شرح می‌دهد. این قسمت همانند قسمت الف-۵ می‌باشد با در نظر داشتن یک استثناء: جملات تطبیق.

جملات تطبیق در رخنمون محافظتی نشان می‌دهد که پگونه مستند هدف اررِیابی و/یا دیگر مستندات رخنمون محافظتی با یک مستند رخنمون محافظتی مطابقت دارند. نویسنده رخنمون محافظتی با انتخاب اینکه ادعای تطبیق محدود (Strict) و یا قابل اثبات (Demonstrable) مورد نیاز است حالتی را انتخاب می‌کند. پیوست «د» را مطالعه کنید.

ب-٦ تعریف مسئله امنیتی (APE_SPD)[3]

محتوای این قسمت به طور کامل در قسمت «الف-۷» بیان شده است.

ب-۷ اهداف امنیت ASE_OBJ [4]

محتوای این قسمت به طور کامل در قسمت «الف -۷ » بیان شده است.

ب-۸ مولفه‌های اضافی تعریف شده ASE_ECD [5]

محتوای این قسمت به طور کامل در قسمت «الف -۸ » بیان شده است.

ب-۹ نیازمندی‌های امنیتی ASE_REQ

محتوای این قسمت به طور کامل در قسمت «الف-۹ » بیان شده است.

1-Requierd NoN-TOE hardware/software/firmware

2 - Conformance Claims

3- Security Problem Definition

4- Security Objectives

5- Extended Component Defenition

توجه داشته باشید که وظایفی که برای تکمیل عملیات در رخنمون محافظتی اندکی متفاوت با آنچه در مستند هدف امنیتی بیان شده است، می‌باشد. این مسئله در قسمت ۸-۱ از این استاندارد بیان شده است.

ب-۱۰ ویژگی‌های TOE[1]

محتوای این قسمت به طور کامل در قسمت «الف-۹ » بیان شده است.

ب-۱۱ مستندات هدف امنیتی با حداقل ضمانت[2]

رخنمون محافظتی با حداقل ضمانت همان رابطه ای را با رخنمون محافظتی معمولی دارد که مستند هدف امنیتی بیان شده در پیوست «الف» داشته است. قسمتهای مختلف رخنمون محافظتی با حداقل ضمانت شامل:

- مقدمه رخنمون محافظتی، شامل مرور بر محصول مورد ارزیابی و مراجع رخنمون محافظتی
- ادعای تطبیق
- اهداف امنیتی برای محیط عملیاتی پیرامون محصول
- نیازمندی‌های عملکردی امنیت و نیازهای ضمانت امنیت (شامل مولفه‌های اضافی تعریف شده) و شمای نیازمندی‌های امنیت (فقط اگر وابستگی برآورده نشده باشد)

یک مستند پرفایل محافظتی با حداقل سطح ضمانت و حتی یک رخنمون محافظتی معمولی، ممکن است ادعای تطبیق خود را بر یک مستند رخنمون محافظتی دیگر با حداقل سطح ضمانت بیان کند.

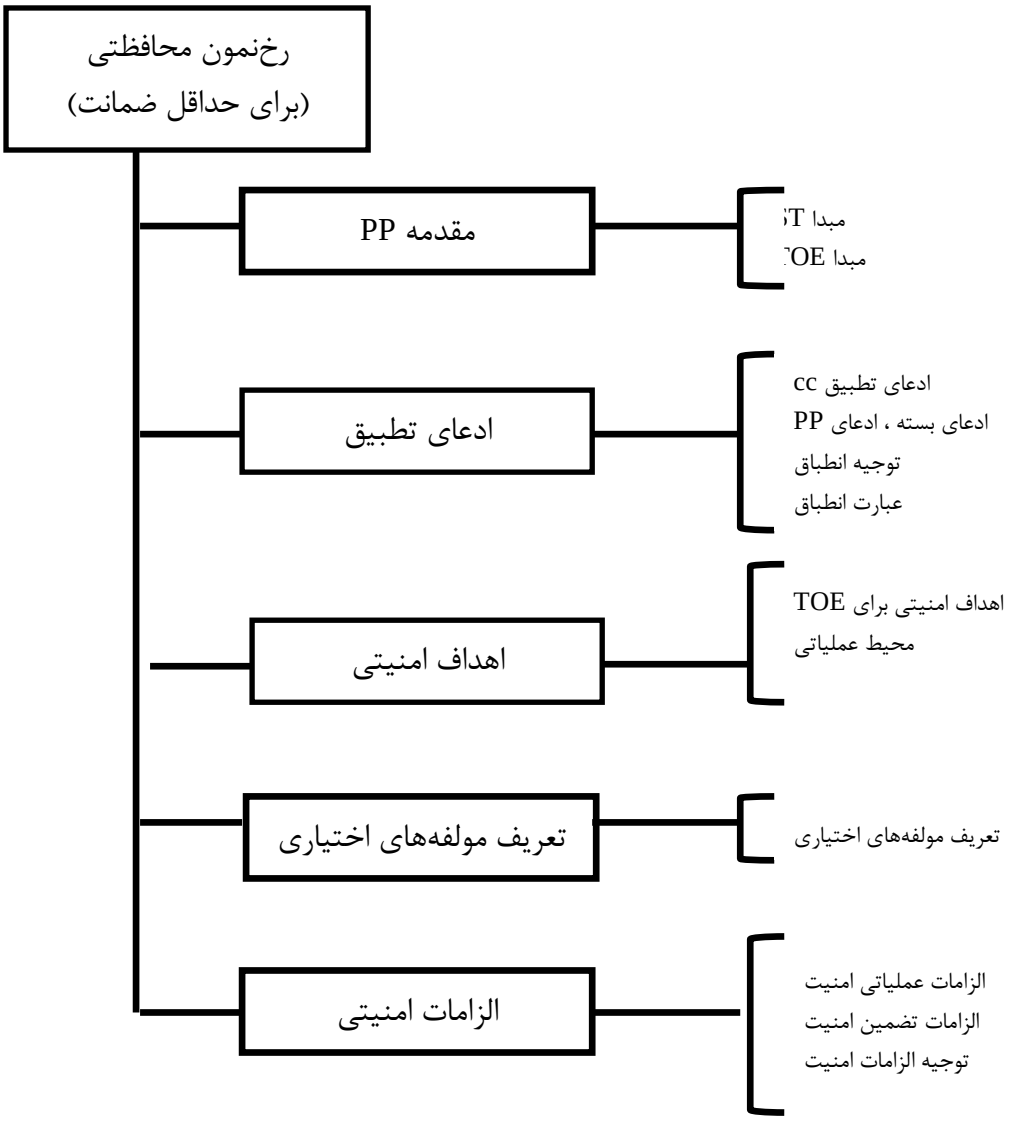
شکل ۱۰ محتوای کاهش یافته از مستند رخنمون محافظتی با حداقل ضمانت بیان می‌کند.

ب-۱۲ ارجاع به دیگر استانداردها در یک مستند هدف امنیتی

این قسمت بیان همان مفادی است که در ضمیمه الف عنوان شده است، با در نظر داشتن یک استثناء: هرگاه که یک رخنمون محافظتی شامل قسمت توصیف خلاصه محصول مورد ارزیابی نباشد، سومین خصیصه بیان شده در قسمت «الف.۱۳» برای این نوع مستندات رخنمون محافظتی مجاز نیست.

نویسنده رخنمون محافظتی باید در نظر داشته باشد که ارجاع به یک استاندارد در مستندات نیازمندی‌های عملکردی ممکن است منجر به تحمیل کردن مسئولیت سنگین ساخت محصولات منطبق بر ضوابط رخنمون محافظتی (با توجه به میزان سطح امنیت مورد نیاز و پیچیدگی و اندازه استاندارد)شود، و این مسئله ممکن است مناسب تر از نیاز به تهیه راه حل‌های غیر مرتبط با ISO/IEC 15408 برتی ارزیابی تطبیق استاندارد باشد.

1- TOE Summary Specification
2- LOW Assurance Protection Profiles



شکل ب-۲ محتوای کاهش یافته از مستند هدف امنیتی با حداقل ضمانت

پیوست پ

(اطلاعاتی)

راهنمایی برای عملیات

پ-۱ معرفی

همانگونه که در قسمت اول استاندارد ISO/IEC 15408 توضیح داده شده است، مستندات رخ‌نمون محافظتی و هدف امنیتی شامل الزامات امنیتی پیش تعریف شده است. از سوی دیگر نویسندگان مستندات رخ‌نمون محافظتی و هدف امنیتی با استفاده از تهیه فهرست‌های مولفه‌های توسعه یافته، قادر به انجام عمل مشابهی هستند.

پ-۲ نمونه‌هایی از عملیات

چهار عملی که در قسمت ۷-۱ تعریف شده است در قسمت ذیل با ذکر مثال‌هایی توضیح داده می‌شوند.

پ-۲-۱ عملیات تکرار

همانگونه که در قسمت ۷-۱-۱ توضیح داده شده است، عملیات تکرار بر روی هر مولفه ای می‌تواند اجرا شود. نویسندگان PP/ST عملیات تکرار را به جهت وجود مجموعه زیادی از نیازمندی‌ها بر روی یک مولفه به کار می‌گیرند. هر تکرار مولفه نسبت به هر تکرار دیگر مولفه متفاوت است، از طرفی این عملیات توسط عملیات تخصیص و انتخاب و/یا توسط به کارگیری عملیات پایش به روش دیگری قابل تکمیل است. تکرارها با تعریف منحصر به فرد شماهای شفاف و دنباله گیری آن از سوی نیازمندی‌ها را مجاز می‌دارد.

یک مثال از عمل تکرار FCS_COP.1 است، عملیات رمزنگاری بنا بر نیاز به پیاده سازی دو الگوریتم مختلف رمزنگاری دوبار تکرار می‌شود. یک مثال از تعریف تکرار منحصر به فرد در ادامه ذکر می‌شود:

عملیات رمزنگاری (RSA و DSA)((FCS_COP.1(1))

عملیات رمزنگاری (TLS/SSL)((FCS_COP.1(2))

پ-۲-۲ عملیات تخصیص

همانطور که در قسمت ۷-۱-۲ توضیح داده شده است، عملیات تخصیص زمانی اتفاق می‌افتد که یک مولفه شامل عنصری باشد که پارامترهای آن توسط نویسنده PP/ST قابل مقدار گذاری باشد. پارامترها می‌توانند مقدار نامحدود بگیرند، یا محدوده ای ازمقادیر تعریف گردد.

یک مثال از یک عنصر در تخصیص FIA_AFL.1.2 است. زمانی که تعدادی از تلاشهای ناموفق احراز هویت تعیین شده اتفاق بیافتد، TSF باید {تخصیص: فهرست از عملیات}

پ-۲-۳ عملیات انتخاب

همانطور که در بخش ۷-۱-۳ توضیح داده شده است، عملیات انتخاب زمانی اتفاق می‌افتد که مولفه داده شده شامل عناصری باشد که نویسنده PP/ST انتخابی از مجموعه داشته باشد.

برای مثال یک عنصر دارای عمل انتخاب FPE_TST.1.1 است. بدین معنا که "TSF باید مجموعه مناسبی از خود آزمون‌ها را اجرا کند {انتخاب: در حین شروع اولیه، بصورت دوره ای در اجرای نرمال، بنا بر تقاضای کاربر

مجاز، بنا بر شرایط(تخصیص: شرایطی که تحت آن باید خودآزمون صورت گیرد) برای نشان داده عملیات صحیح و ..}"

پ-۲-٤ عملیات پایش

همانگونه که در بخش ۷-۱-۴ توضیح داده شده است عملیات پایش بر روی همه نیازمندی‌ها قابل اجرا است. نویسنده PP/ST این عمل را با جایگزینی نیازمندی‌های مناسب تر انجام می‌دهد.

مثالی از عمل پایش معتبر، FIA_UU.2.1 است، که بیان می‌کند«TSF باید الزام بر احراز هویت موفق همه کاربران قبل از اجرای عملیات مجاز توسط کاربران در TSF دارد» پایش این عمل به این صورت است که «TSF باید الزام بر احراز هویت موفق همه کاربران از طریق نام کاربری و گذرواژه قبل از اجرای عملیات مجاز توسط کاربران در TSF دارد»

اولین نقش عملیات پایش این است که محصول مورد ارزیابی نیازمندی‌های پایش شده و همچنین نیازمندی‌های پایش نشده در محتوای PP/ST برآورده سازد. (برای مثال الزامات پایش شده محدود تر از الزامات معمولی هستند).

تنها استثنا در این نقش این است که نویسنده PP/ST مجاز به پایش نیازمندی‌های عملکردی امنیت برای به کارگیری در بخشی و نه همه موضوعات، اهداف و عملیات و ویژگی‌های امنیتی داخلی و خارجی است.

یک مثال از چنین استثنائی FIA_UAU.2.1 است، که بیان می‌دارد«TSF باید الزام بر احراز هویت موفق همه کاربران قبل از اجرای عملیات مجاز توسط کاربران در TSF دارد » و پایش شده این مولفه اینگونه است که « TSF باید الزام بر احراز هویت موفق همه کاربران فضای اینترنت قبل از اجرای عملیات مجاز توسط کاربران در TSF دارد ».

دومین نقض عملیات پایش این است که عملیات پایش باید با مولفه اصلی اولیه در ارتباط باشد. برای مثال پایش یک مولفه کلاس ممیزی با ایجاد عنصر اضافی در جلوگیری از امواج الکترومغناطیس مجاز نیست.

یک حالت خاص از عملیات پایش پایش ویرایشی است، به گونه ای که تغییر کوچک در نیازمندی ایجاد می‌شود.برای مثال بازنویسی یک جمله به دلیل تبعیت صحیح از قواعد زبان انگلسی یا ایجاد فهم بیشتر برای خوانندگان. ایجاد این تغییرات به معنای تغییر معنا و مفهوم نیازمندی تحت هیچ شرایطی نیست. برخی از پایش‌های ویرایشی شامل:

نیازمنیدی عملکردی امنیت FPT_FLS.1 که بیان می‌دارد «TSF باید وضعیت امن را زمانی که خطاهای خراب شدن یک پردازنده اتفاق افتاد حفظ کند، » این نیازمندی می‌تواند اینگونه تغییر کند که «TSF باید وضعیت امن را در زمان از بین رفتن یک پردازنده همچنان حفظ کند، »

پ-۳ سازماندهی مولفه‌ها

استاندارد ISO/IEC 15408 سازماندیه مولفه‌های قسمت دوم و سوم را به شکل ساختار سلسله مراتبی زیر بیان کرده است:

کلاسها، شامل

- خانواده‌ها، شامل
- مولفه‌ها، شامل

- عناصر

سازماندهی به شکل سلسله مراتبی ، کلاس – خانواده – مولفه – عنصر برای کمک به مشتریان و توسعه دهندگان و ارزیابان است تا بتوانند مولفه مورد نظر خودشان را به راحتی مشخص کنند.
استاندارد ISO/IEC 15408 الزامات عملکردی و ضمانتی امنیت را تحت یک ساختار مشابه سلسله مراتبی ارائه می‌کند، و یک مجموعه لغات و ساختار برای هر دو استفاده می‌کند.

پ-۳-۱ کلاس

یک مثال از کلاس FIA است. کلاس تشخیص و احراز هویت، که بر شناسایی کابران و احراز هویت آنها و مقید سازی کاربران بر موضوعات تمرکز دارد.

پ-۳-۲خانواده

یک مثال از خانواه ، احراز هویت کاربر یعنی (FIA_UAU) است. که در حقیقت قسمتی از کلاس FIA می‌باشد. این خانواده بر احراز هویت کاربران تمرکز دارد.

پ-۳-۳ مولفه

یک مثال از مولفه FIA_UAU.3 است، احراز هویت دائمی که بر از بین نرفتن موارد احراز هویت شده تمرکز دارد.

پ-۳-٤ عنصر

یک مثال از عنصر FIA_UAU.3.2 است که تمرکز بر جلوگیری از کپی کردن اطلاعات احراز هویت دارد.

پ-٤ مولفه‌های توسعه یافته

پ-٤-۱چگونگی تعریف مولفه‌های توسعه یافته

هرگاه یک نویسنده PP/ST مولفه توسعه یافته ای را تعریف کند، باید همانند دیگر مولفه‌های موجود در ISO/IEC 15408 رفتاری مشابه انجام دهد: شفاف و غیر مبهم و قابل ارزیابی . مولفه‌های توسعه یافته باید همانند دیگر مولفه‌ها برچسب گذاری شوند، رفتارشان بیان شود و در همان سطحی که استاندارد ISO/IEC 15408 جزئیات را بیان می‌کند، تفصیلی باشند.
نویسنده PP/ST باید اطمینان حاصل کند که همه وابستگی‌هایی که قابلیت به کارگیری در مولفه توسعه یافته دارند در قسمت تعریف مولفه توسعه یافته گنجانده شده است. مثال‌هایی از وابستگی‌های ممکن عبارتند از:

- اگر یک مولفه توسعه یافته به ممیزی ارجاع داشته باشد، وابستگی به کلاس FAU، کلاس ممیزی امنیت ممکن است گنجانده شود
- اگر مولفه توسعه یافته داده ای را تغیر دهد یا دسترسی پیدا کند، وابستگی به مولفه سیاست کنترل دستری FDP_AISO/IEC 15408 پیدا کرده خانواده‌های آن ممکن است به کار روند.
- اگر مولفه توسعه یافته از یک توصیف طراحی خاص برگرفته از کلاس توسعه ADV باشد، خانواده کلاس توسعه ممکن است گنجانده شود.

در مورد مولفه‌های عملکردی توسعه یافته، نویسنده PP/ST همچنین باید شامل هر اطلاعات عملیات مشارکت یا ممیزی در تعریف آن مولفه مشابه آنچه در قسمت دوم استاندارد ISO/IEC 15408 است، بگنجاند.

در مورد نیازهای ضمانت امنیت نویسنده PP/ST باید متدولوژی ارزیابی مناسب همانند CEM را تهیه کند.
مولفه‌های توسعه یافته ممکن است در خانواده‌های موجود گنجانده شوند، در این مورد نویسنده PP/ST باید چگونگی تغییر این مولفه‌ها را بیان کند. اگر این مولفه‌های توسعه یافته مناسب جایگزینی خانواده‌های موجود نباشند، باید بعنوان خانواده‌های جدید تعریف شوند. تعریف خانواده جدید هم میبایست کاملا منطبق با خانواده‌های تعریف شده ISO/IEC 15408 باشد.
خانواده‌های جدید ممکن است در کلاسهای موجود درج شوند بطوری که نویسنده PP/ST چگونگی تغییر این کلاسهای را بیان کند. اگر این کلاس‌های توسعه یافته مناسب جایگزینی کلاسهای موجود نباشند، باید بعنوان کلاسهای جدید تعریف شوند. تعریف کلاس جدید هم باید کاملا منطبق با خانواده‌های تعریف شده ISO/IEC 15408 باشد.

پیوست ت

(اطلاعاتی)
تطبیق رخ‌نمون محافظتی

ت-۱ معرفی

مستند رخ‌نمون محافظتی بعنوان یک الگو برای مستند هدف ارزیاب در نظر گرفته می‌شود. بدین معنا که، رخ‌نمون محافظتی مجموعه ای از نیازهای کاربر را تعریف کرده در حالی که مستند هدف امنیتی فقط مطابعت محصول مورد ارزیابی از نیازهای بیان شده در رخ‌نمون محافظتی را نشان می‌دهد.

توجه داشته باشید که ممکن است یک مستند رخ‌نمون محافظتی بعنوان الگویی برای مستند رخ‌نمون محافظتی دیگر در نظر گرفته شود. این بدین معنا است که یک PP می‌تواند ادعای انطباق با یک PP دیگر را داشته باشد. این مسئله کاملا مشابه مطابقت ST با PP است. برای وضوح بیشتر در این پیوست فقط به شرح حالت ST/PP می‌پردازیم در حالی که امکان استفاده برای PP/PP هم وجود دارد.

استاندارد ISO/IEC 15408 هیچ نوع مطابقت جزئی را مجاز نمی دارد، بنابراین اگر اظهار انطباق با یک مستند رخ‌نمون محافظتی وجودداشته باشد، مستندات اهداف ارزیابی یا رخ‌نمون محافظتی ادعا کننده باید به طور کامل همه مراجع آن را برآورده سازند. هرچند دو مدل مختلف از انطباق وجوددارد (محض، قابل اثبات) و نوع انطباق مجاز توسط مستند رخ‌نمون محافظتی بیان می‌شود. این مسئله در قسمت جملات انطباق PP در «ب.۵»بیان شده است که چه نوع مطابقت‌هایی برای مستندات هدف امنیتی مجاز هستند. فاصله بین مطابقت محض وقابل اثبات بر روی هر مستند رخ‌نمون محافظتی قابل اعمال است، به گونه ای که هر مستد هدف امنیتی برای هر قسمت مجزا می‌تواند ادعای تطبیق را بیان کند. بعبارت دیگر مستند هدف امنیتی می‌تواندمطابقت محض با برخی از رخ‌نمون‌های محافظتی داشته باشد وبا برخی دیگر مطابقت قابل اثبات داشته باشد. مطابقت قابل اثبات فقط در مواردی مجاز است که اولا رفتار مستند هدف امنیتی قابل اثبات باشد که همانند رفتار PP است و از طرف دیگر مستند PP این نوع مطابقت را مجاز دانسته باشد. ولی مطابقت محض همواره قابل بیان است.

بعبارت دیگر، یک مستند هدف امنیتی فقط مجاز به بیان ادعای تطبیق از نوع رفتار قابل اثبات دارد به شرطی که مستند رخ‌نمون محافظتی این مسئله را صریحا مطرح کرده باشد.

مطابقت به معنای برآورده ساختن همه الزاماتی است که PP بیان کرده است. رخ‌نمون‌های محافظتی منتشر شده به طور معمول نیاز به مطابقت قابل اثبات دارند، به این معنا که مستند هدف امنیتی برای اثبات تطابق خود کافی است، راه حلی را برای مسئله امنیتی مطرح شده در PP بیان کند، هر چند برای انجام این مسئله می‌تواند از هر راهی که معادل یا بسیار سخت گیرانه تر از روند مطرح شده در PP باشد، استفاده کند. معادل بودن یا بسیار سخت گیرانه بودن در طول استاندارد ISO/IEC 15408 تعریف شده اند، اما بصورت مفهومی بدین معنا است که مستد PP مستند ST ممکن است در نهایت از جملات متفاوتی که بر هستارهای مختلفی بحث می‌کند و حتی مفاهیم مختلف و غیره استفاده کرده باشند. مستند هدف امنیتی محدودیت‌های مشابه آنچه PPذکر داشته یا بیشتر از آن را بر محصول مورد ارزیابی و به همان اندازه یا کمتر را برای محیط عملیات پیرامون محصول مورد ارزیابی ارائه کند.

ت-۲ مطابقت محض

مطابقت محض منوط به شواهد و ادله مورد نیاز برای اثبات برآورده شده الزامات PP است به همان گونه ای که نویسنده PP مطرح ساخته است. بدین ترتیب مستند هدف امنیتی یک شمایی از مستند رخنمون محافظتی است هرچند مستند هدف امنیتی می‌تواند گسترده تر از رخنمون محافظتی باشد. به طور ذاتی مستند هدف امنیتی حداقل الزاماتی را بیان می‌کند که محصول مورد ارزیابی باید از رخنمون محافظتی برآورده سازد. در حالی که محیط عملیاتی پیرامون باید همان طوری باشد که مستند رخنمون محافظتی عنوان کرده است.

یک مثال از استفاده مطابقت محض این است که قصد تهیه محصولی را داریم که دقیقا نیازمندی‌های مندرج در یک رخنمون محافظتی را برآورده سازد، در این صورت انطباق محض تنها راه نشان دادن وجود همه خصیصه‌های امنیتی مورد درخواست در محصول می‌باشد.

معرفی یک مستند هدف امنیتی با عنوان مطابقت محض با یک رخنمون محافظتی می‌تواند محدودیت‌های بیشتر از آنچه که در PP ارائه شده را معرفی کند.

ت-۳ مطابقت قابل اثبات

مطابقت قابل اثبات، منوط به بیان راه حل مناسب برای حل مسئله امنیتی بیان شده در رخنمون محافظتی می‌باشد به همان گونه ای که نویسنده PP بیان داشته است.

از آنجایی که رابطه زیر مجموعه ای بین مستند هدف امنیتی و مستند رخنمون محافظتی در حالت مطابقت محض وجود دارد، رابطه این دو مستند در حالت تطابق قابل اثبات به این روشنی نیست. مستندهای اهداف ارزیابی که ادعای انطباق قابل اثبات را با مستند رخنمون محافظتی دارند، باید، راه حلی برای رفع مسئله امنیتی توصیف شده در رخنمون محافظتی بیان دارند، اما برای نشان دادن این اثبات، روش انتخابی می‌تواند معادل یا محدود تر از آنچه که در PP عنوان شده است استفاده کند.