به نام خدا

پروفایل حفاظتی تجهیزات شبکه بی‌سیم

نسخه ۱,۵

اردیبهشت ماه ۹۳

پیش‌گفتار

این سند توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است که معرفی کننده الزامات کارکرد امنیتی برای تجهیزات شبکه بی‌سیم می‌باشد تا تولیدکنندگان محصولات تجهیزات شبکه بی‌سیم بتوانند بر مبنای این سند، کارکردهای امنیتی را در محصول خود لحاظ و سند هدف امنیتی آن را ارائه کنند.

در بخش اول به معرفی این دسته از تجهیزات پرداخته شده است. سپس در بخشی تحت عنوان «مسائل امنیتی»، تهدیدهایی که محصول با آنها روبرو است و فرضیاتی که در رابطه با امنیت محصول در نظر گرفته شده است و همچنین خط‌مشی‌های آن عنوان می‌شود.

سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدها، اجرای خط مشی‌ها و بکاربردن فرضیات مطرح می‌شود.

در بخش بعدی «الزامات کارکرد امنیتی آورده شده است. براساس استاندارد معیار مشترک این قسمت از چندین کلاس تشکیل شده است که هریک از این کلاس‌ها حوزه خاصی از امنیت را پوشش می‌دهند. کلاس‌هایی که برای تجهیزات شبکه بی‌سیم در این سند مطرح شده‌اند، عبارتند از:

- کلاس ممیزی امنیت
- کلاس پشتیبانی از رمزنگاری
- کلاس حفاظت از داده‌های کاربری
- کلاس شناسایی و احراز هویت
- کلاس مدیریت امنیت
- کلاس حفاظت از توابع امنیتی هدف ارزیابی
- کلاس دسترسی به هدف ارزیابی
- کلاس تخصیص منابع
- کلاس کانال‌ها / مسیرهای مورد اعتماد

هر کلاس مجموعه‌ای از خانواده و هر خانواده مجموعه‌ای از مولفه و هر مولفه مجموعه‌ای از عناصر می‌باشد. با استفاده از «الزامات کارکرد امنیتی» در واقع «اهداف امنیتی» بر مبنای استاندارد معیار مشترک بیان می‌گردد.

در بخش پایانی «الزامات تضمین امنیتی» که از ساختاری مشابه بخش قبلی برخوردار است مطرح گردیده است، این بخش الزامات لازم جهت ارزیابی محصول را عنوان می‌نماید.

فهرست

۱ هدف از ارائه سند

در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک لازم است تا الزامات کارکرد امنیتی هر محصول بیان شود. بیان این الزامات برای توسعه دهندگان محصولات این مزیت را خواهد داشت تا راهکارهایی را که در این سند برای برآورده نمودن الزامات ارائه شده‌اند، در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک خواهد کرد.

۲ معرفی اصطلاحات

- **هدف ارزیابی (TOE)**

به سامانه مورد ارزیابی براساس «استاندارد ارزیابی معیار مشترک»، هدف ارزیابی گفته می‌شود.

- **غیر هدف ارزیابی (Non-TOE[1])**

سخت‌افزار، نرم‌افزار و میان افزاری که هدف ارزیابی جهت اجرا به آن‌ها نیز نیاز دارد.

- **محیط عملیاتی (Operational Environment)**

محیطی که هدف ارزیابی در آن عمل می‌کند.

- **پروفایل حفاظتی (PP[2])**

بیانیه‌ی الزامات امنیتی برای یک نوع از هدف ارزیابی، که الزامات امنیتی را به صورت کلی بیان می‌کند.

[1] Non-Target Of Evaluation

[2] Protection Profile

- **هدف امنیتی (ST[1])**

بیانیه الزامات امنیتی برای هدف ارزیابی خاصی، که الزامات امنیتی را به صورت جزئی‌تر بیان می‌دارد. این بیانیه معمولاً توسط سازنده هدف ارزیابی نوشته می‌شود.

- **مسائل امنیتی (Security Problem)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «مشکل امنیتی» وجود دارد که به طور رسمی ماهیت و حوزه امنیت در نظر گرفته شده توسط هدف ارزیابی را تعریف می کند.

این بیانیه شامل موارد زیر است:

- «تهدیدهایی» که توسط هدف ارزیابی و محیط عملیاتی‌اش مقابله می‌شود.
- «خط‌مشی امنیت سازمانی» که توسط هدف ارزیابی و محیط عملیاتی‌اش اجرا می‌شود.
- «فرضیاتی» که برای محیط عملیاتی هدف ارزیابی تائید می‌شوند.

- **عامل تهدید (Threat Agent)**

موجودیت‌هایی که می‌توانند بر روی دارایی‌ها اقدام تهاجمی انجام دهند.

- **خط‌مشی امنیتی سازمانی (OSP[2])**

مجموعه‌ای از قوانین، که توصیف کننده رفتار امنیتی خاصی است که توسط «توابع امنیتی هدف ارزیابی» اجرا می‌شوند؛ این مجموعه قوانین به صورت یک مجموعه از «الزام‌های کارکرد امنیتی» قابل بیان است.

[1] Security Target

[2] Organizational Security Policy

- **اهداف امنیتی (Security Objective)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «اهداف امنیتی» وجود دارد که برای مقابله با تهدیدهای معرفی شده و/یا برای برآورده کردن خط‌مشی‌های امنیت سازمان و یا فرضیات معرفی شده در بخش «مسائل امنیتی»، در نظر گرفته شده است.

- **الزام امنیتی (Security Requirement)**

الزاماتی که به زبان استاندارد بیان می‌شوند تا در حصول اهداف ارزیابی، برای هدف ارزیابی کمک کنند.

- **الزام کارکرد امنیتی (SFR[1])**

بیان کننده کارکردهای امنیتی هدف ارزیابی در قالب کلاس است. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام کارکرد امنیتی» وجود دارد.

- **الزامات تضمین امنیتی (SAR[2])**

این دسته از الزامات اطمینان می‌دهند که الزامات کارکرد امنیتی توسط هدف ارزیابی برآورده می‌شوند. در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «الزام تضمین امنیتی» وجود دارد.

- **بسته (Package)**

نام مجموعه‌ای از الزامات کارکرد امنیتی یا تضمین امنیتی است. به عنوان مثال EAL3.

[1] Security Functional Requirement

[2] Security Assurance Requirement

- **سطح تضمین ارزیابی (EAL[1])**

مجموعه‌ای از الزامات تضمین که از قسمت سوم از سندهای سه‌گانه «استاندارد ارزیابی معیار مشترک» برگرفته شده است و نشان دهنده سطح امنیتی محصول می‌باشد. سطوح تضمین از سطح ۱ تا سطح ۷ هستند، لازم به ذکر است که «سطح تضمین امنیتی» یک نوع «بسته» می‌باشد.

- **توابع امنیتی هدف ارزیابی (TSFs[2])**

آن بخش از هدف ارزیابی که برای اجرای صحیح «الزامات کارکرد امنیتی» باید به آن تکیه کرد، به عنوان «توابع امنیتی هدف ارزیابی» نام برده می‌شود. «توابع امنیتی هدف ارزیابی» شامل تمام سخت‌افزار، نرم‌افزار و میان‌افزارهای هدف ارزیابی است که مستقیم و غیرمستقیم برای اجرا شدن امنیت باید به آنها تکیه کرد.

- **داده توابع امنیتی هدف ارزیابی (TSF data)**

داده‌هایی برای عملیات هدف ارزیابی هستند که اجرای الزامات کارکرد امنیتی وابسته به آنها است. این داده‌ها اطلاعات استفاده شده توسط توابع امنیتی هدف ارزیابی هستند.

- **داده کاربری (User data)**

داده‌های کاربری هستند که عملکرد توابع امنیتی هدف ارزیابی را تحت تاثیر قرار نمی‌دهند. این داده‌ها اطلاعاتی ذخیره شده در منابع هدف ارزیابی هستند که توسط کاربران مطابق با الزامات کارکرد امنیتی به کار برده می‌شوند. محتویات یک پیام الکترونیک نوعی داده کاربری می‌باشد.

- **کلاس (Class)**

1 Evaluation Assurance Level

2 TOE Security Functions

مجموعه‌ای از خانواده‌های «استاندارد ارزیابی معیار مشترک» که روی یک موضوع متمرکز، اشتراک دارند.

- **خانواده (Family)**

مجموعه‌ای از عناصر که بر روی یک هدف اشتراک دارند اما در دقت و میزان تاکید، تفاوت دارند.

- **عنصر (Component)[۱]**

کوچکترین مجموعه از مؤلفه‌های قابل انتخاب، که الزامات ممکن است براساس آن‌ها باشد.

- **مؤلفه (Element)[۲]**

بیانی از نیاز امنیتی که غیر قابل تجزیه است.

- **اختصاص (Assignment)**

مشخص نمودن پارامترهای معرفی شده در یک مؤلفه (از استاندارد معیار مشترک) یا الزام است.

- **انتخاب (Selection)**

انتخاب یک یا بیش از یک آیتم در لیستی که در مؤلفه یا الزام وجود دارد.

- **سرپرست (Administrator)**

[۱] **در استاندارد ملی** ISO 15408 **منتشر شده توسط سازمان ملی استاندارد ایران،** Component **مولفه ترجمه شده است.**

[۲] **در استاندارد ملی** ISO 15408 **منتشر شده توسط سازمان ملی استاندارد ایران،** Element **عنصر ترجمه شده است.**

موجودیتی که مسئولیت مدیریت و اعمال خط‌مشی‌ها را بر روی هدف ارزیابی بر عهده دارد و معمولا دارای بالاترین سطح مجوز است.

- **موجودیت فعال (Subject)**

موجودیت فعال، موجودیتی در سامانه مورد ارزیابی (هدف ارزیابی) است که عملیاتی را بر روی موجودیت‌های غیرفعال انجام می‌دهد. همانند نقش‌هایی همچون سرپرست، کاربر نهایی و غیره. به عبارت دیگر موجودیت فعال عامل انجام عملی بر روی هدف ارزیابی است.

- **موجودیت غیرفعال (Object)**

موجودیت غیرفعال، موجودیتی در سامانه مورد ارزیابی (هدف ارزیابی) می‌باشد که شامل اطلاعات است و یا اطلاعات را دریافت می کند و روی آن توسط موجودیت‌های فعال، عملیاتی انجام می‌گیرد. همانند داده‌ها و اطلاعاتی همچون متن‌های رمز شده و کلیدها و غیره. به عبارت دیگر موجودیتی است که توسط موجودیت فعال بر روی آن رخدادی اتفاق می‌افتد، مانند لیست کردن رکوردها توسط سرپرست، حذف فایل‌ها توسط حمله کننده که در این دو مثال رکوردها و فایل‌ها موجودیت‌های غیرفعال هستند.

- **راز (Secret)**

اطلاعاتی که باید تنها به کاربران مجاز و/یا توابع امنیتی هدف ارزیابی شناسانده شود تا یک «خط‌مشی کارکرد امنیتی » اجرا شود.

- **مشخصه امنیتی (Security Attribute)**

کاربران، موجودیت‌های فعال، اطلاعات، موجودیت‌های غیرفعال، نشست‌ها و منابع تحت کنترل قوانین «الزامات کارکرد امنیتی» ممکن است دارای اطلاعات خاصی باشند که جهت کارکرد صحیح هدف ارزیابی، مورد استفاده قرار گیرند. دسته‌ای از این اطلاعات حالت آگاهی‌دهنده دارند هم‌چون نام فایل که ممکن است برای معرفی منابع منحصر به فرد استفاده شود، اما دسته‌ی دیگر از این اطلاعات ممکن است به طور خاص برای اجرا شدن الزامات کارکرد امنیتی وجود داشته باشند، همانند اطلاعات کنترل دسترسی، این دسته از اطلاعات به طور کلی «مشخصه امنیتی» نامیده می‌شود.

- **خط‌مشی کارکرد امنیتی (SFP[1])**

رفتار امنیتی که توسط «کارکرد امنیتی هدف ارزیابی» اجرا می‌شوند تحت مجموعه قوانینی در «الزامات کارکرد امنیتی» بیان می‌شوند. این مجموعه قوانین «خط مشی کارکرد امنیتی» نامیده می‌شوند. «الزامات کارکرد امنیتی» ممکن است چندین خط‌مشی جهت معرفی قوانینی که هدف ارزیابی باید اجرا کند، تعریف کند. هر کدام از خط‌مشی‌ها باید حوزه کنترلی‌اش را توسط موجودیت‌های فعال، موجودیت‌های غیرفعال، منابع یا اطلاعات و عملکردهایی که بکار برده است، مشخص کند. تمام این خط‌مشی‌ها توسط «توابع امنیتی هدف ارزیابی» پیاده‌سازی می‌شوند.

- **خط‌مشی کارکرد امنیتی کنترل دسترسی (Access Control SFP)**

چندین خط‌مشی کارکرد امنیتی وجود دارد که برای حفاظت از داده‌ها بکار برده می‌شوند، همچون «خط‌مشی کنترل دسترسی» و «خط مشی کنترل جریان اطلاعات». «خط‌مشی کنترل دسترسی» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی کاربران، منابع، موجودیت‌های فعال، موجودیت‌های غیرفعال، نشست‌ها، TSF status data و عملکردها در حوزه کنترلی‌شان پیاده‌سازی می‌شوند.

این مشخصه‌های امنیتی در مجموعه قوانینی استفاده می‌شوند که حاکم بر عملیاتی است که موجودیت‌های فعال ممکن است بر روی موجودیت‌های غیرفعال اجرا کنند.

- **خط‌مشی کنترل جریان اطلاعات (Information Flow Control SFP)**

«خط‌مشی جریان اطلاعات» مکانیزم‌هایی هستند که براساس احکام خط‌مشی‌هایشان، بر روی مشخصه‌های امنیتی موجودیت‌های فعال و اطلاعات در حوزه کنترلی‌شان و مجموعه قوانین حاکم بر عملیات که توسط موجودیت فعال بر روی اطلاعات صورت می‌گیرد، پیاده‌سازی می‌شوند.

1 Security Functionality Policy

۳ معرفی استاندارد ۱۵۴۰۸

استاندارد ISO/IEC 15408 که به عنوان استاندارد ارزیابی معیار مشترک[1]نیز شناخته می‌شود با هدف تعیین مبنایی جهت ارزیابی ویژگی‌های امنیتی محصولات فناوری اطلاعات و سیستم‌ها تدوین گردیده است. با ایجاد چنین مبنایی با معیار مشترک، نتایج ارزیابی امنیتی فناوری اطلاعات برای تعداد بیشتری از مخاطبین حائز اهمیت خواهد بود.

استاندارد ISO/IEC 15408 در برگیرنده مولفه‌های عملکرد امنیتی بوده که مبنایی برای ارزیابی الزامات عملکرد امنیتی موجود در پروفایل حفاظتی[2]یا هدف امنیتی[3]است.

این الزامات به توضیح رفتارهای امنیتی مورد نظر هدف ارزیابی[4]یا محیط فناوری اطلاعات پرداخته و هدف آن برآورده نمودن اهداف امنیتی که در پروفایل حفاظتی یا هدف امنیتی تعیین شده است، می‌باشد.

استاندارد ISO/IEC 15408 در سه بخش ارائه شده است :

بخش اول: مقدمه و مدل عمومی (اصطلاحات و واژگان)

بخش دوم: الزامات کارکرد امنیتی [5]

بخش سوم: الزامات تضمین امنیتی [1]

---

[1] Common Criteria (CC)

[2] Protection Profile (PP)

[3] Security Target (ST)

[4] Target Of Evaluation (TOE)

[5] Security Functional Requirement (SFR)

[1] Security Assurance Requrement (SAR)

۴ آشنایی با تجهیزات شبکه محلی بی‌سیم

این سند الزامات کارکرد امنیتی برای سامانه دسترسی WLAN را مشخص می‌کند. سامانه دسترسی WLAN دستیابی بی‌سیم امنی به شبکه کابلی فراهم می‌آورد. این امر توسط کنترل نمودن ارتباط بین کلاینت بی‌سیم و شبکه کابلی صورت می‌گیرد. هدف ارزیابی ممکن است توسط یک یا بیش از یک عنصر فیزیکی پیاده‌سازی شود.

۴,۱ استفاده و ویژگی‌های امنیتی اصلی هدف ارزیابی

سامانه دسترسی WLAN به یک راه‌حل امن دسترسی بی‌سیم برای ایجاد ارتباطی امن بین کاربر(کلاینت بی‌سیم) و شبکه کابلی (به عنوان مثال، شبکه سازمانی) توسط عملکردهای مدیریت متمرکز، کنترل سیاست‌گذاری، سرویس‌های رمزنگاری برای حمایت از سرپرست، احراز هویت، رمزنگاری و حفاظت و مدیریت داده‌های منتقل شده، کمک می‌کند.

سامانه دسترسی WLAN، کلاینت بی‌سیم را ملزم به اجرای احراز هویت 802.1X می‌کند تا با تکیه به سرور احرازهویت پیش از دستیابی به شبکه، کلاینت را احراز هویت کند. سامانه دسترسی WLAN به عنوان مجوزی از طریق تجهیزات بین کلاینت بی‌سیم و سرور احراز هویت عمل می‌کند. تنها در صورتیکه احراز هویت با موفقیت انجام شده باشد، تونل‌های ارتباطی امنی شکل می‌گیرند. در ادامه احرازهویت موفق، سامانه دسترسی WLAN با هر کلاینت بی‌سیم یک کلید نشست ایجاد می‌کند. تمام زیر ارتباطات بین سامانه دسترسی WLAN و کلاینت بی‌سیم رمز شده هستند. سامانه دسترسی WLAN ترافیکی را که از یک کلاینت بی‌سیم احرازهویت شده ایجاد شده است رمزگشایی می‌کند و ترافیک را در داخل شبکه پشتیبانی[1] عبور می‌دهد. به همین ترتیب، سامانه دسترسی WLAN تراقیک ارسال شده را از شبکه پشتیبانی به کلاینت بی-سیم احراز هویت شده، رمز می‌کند.

1 Backend network

سامانه دسترسی WLAN از چندین اتصال بی‌سیم هم‌زمان پشتیبانی می‌کند و قادر به برقراری و پایان دادن به تونل‌های رمزنگاری چندگانه به/از سامانه‌های همتا است.

هدف‌های ارزیابی که مطابق این پروفایل حفاظتی هستند، الزامات ESS را که در استاندارد 802.11 مشخص شده است، با استفاده از احرازهویت 802.1X در برخواهد گرفت. هیچ الزامی وجود ندارد و متعاقباً هیچ ادعای بررسی شده‌ای مربوط به عملکرد IBSS و یا عملکرد ESS که از کلیدهای از پیش مشترک استفاده می‌کنند وجود ندارد.

هدف ارزیابی دارای یک نقش سرپرستی است. سرپرستان باید پیش از آنکه بتوانند هدف امنیتی را مدیریت کنند، احراز هویت شوند. سامانه دسترسی WLAN از هردو سازوکار احرازهویت از راه دور و سازوکار احراز هویت محلی استفاده می‌کند تا ورود سرپرست صورت بگیرد. سرپرست از راه دور می‌تواند به سامانه دسترسی WLAN از طریق یک اتصال امن پیاده سازی شده توسط SSH یا TLS/HTTPS دستیابی داشته باشد(برای مثال). به صورت پیش‌فرض توانایی پیکربندی هدف ارزیابی از سمت بی‌سیم غیرفعال شده است.

چنانچه سامانه دسترسی WLAN توسط دو یا بیش از دو عنصر فیزیکی پیاده‌سازی شود، یک کانال امن بین عناصر هدف ارزیابی برقرار می‌شود تا از تبادل داده کنترل شده/پیکربندی شده بین عناصر محافظت کند. به طور مشابه، موجودیت‌های IT در محیط عملیاتی (سرور RADIUS، سرور ممیزی) به هدف ارزیابی بر روی یک کانال امن مرتبط خواهند شد. تمام موجودیت‌های IT از طریق استفاده از رازهای به اشتراک گذاشته شده یا گواهینامه‌های ماشین X.509v3 جهت احراز هویت، احراز هویت خواهند شد.

فرض شده است که تمام عناصر سامانه دسترسی WLAN به طور مناسب پیاده‌سازی شده است و شامل هیچ نوع اشتباه طراحی حساسی نیست. لازم است که فروشنده راهنمای پیکربندی ارائه دهد (AGD_PRE، AGD_OPR) تا هدف ارزیابی به طور صحیح نصب شود و سرپرست هدف ارزیابی برای هر محیط عملیاتی پشتیبانی شود.

۴,۲ رمزنگاری

انتظار می‌رود سامانه دسترسی WLAN ترافیک جاری بین دو تجهیزی که به طور منطقی از هم مجزا می‌باشند را رمز می¬¬کند. سامانه دسترسی WLAN به عنوان یک نقطه‌ی پایانی برای تونل WLAN به کار می‌رود و تعدادی عملکردهای رمزنگاری مربوط به برقراری و نگهداری تونل را انجام می‌دهد.

اگر رمزنگاری استفاده شده در احراز هویت، کلیدهای تولید شده و اطلاعات رمز شده به اندازه کافی محکم باشد و پیاده‌سازی شامل هیچ اشتباه طراحی حساسی نباشد در این صورت مهاجم قادر به جستجوی فراگیر فضای کلید رمزنگاری جهت به دست آوردن داده‌های بی‌سیم نخواهد بود. مطابق با WPA2 مشخص شده در استاندارد IEEE802.11 و استاندارد IEEE802.1X،یک RBG صحیح و عوامل احراز هویت امن اطمینان می‌دهد که دستیابی به اطلاعات منتقل شده امن نمی‌تواند با تلاشی کمتر از جستجوی کامل فضای کلید به دست آید. هر متن مخفی و کلیدهای خصوصی یا دیگر پارامترهای امنیتی رمزنگاری زمانی‌که دیگر استفاده نمی‌شوند، صفر خواهد شد تا از افشاء داده‌های حساس امنیتی جلوگیری شود.

علاوه بر حفاظت از اطلاعات بی‌سیم، سامانه دسترسیWLAN باید قابلیتی را برای ارتباط امنِ نشست‌های سرپرستی راه دور فراهم کند هم‌چنین از بسته‌های RADIUS بین خود و سرور احراز هویت خارجی محافظت کند.

این معیارها کمک می‌کنند تا از دسترسی غیرمجازِ واسط های خارجی و داخلی از طریق استفاده از احراز هویت همتا، محرمانگی و یکپارچگی داده و پروتکل‌های منطبق جلوگیری شود.

۵ مسائل امنیتی

۵,۱ تهدیدها

T.Type	توضیحات
T.TSF_FAILURE	سازوکارهای امنیتی هدف ارزیابی ممکن است با شکست مواجه شود و منجر به خطر افتادن توابع امنیتی هدف ارزیابی شود.
T.ADMIN_ERROR	در صورت نصب و پیکربندی نامناسب هدف ارزیابی توسط سرپرست، ممکن است سازوکارهای امنیتی کارایی لازم را نداشته باشند.
T.UNAUTHORIZED_ACCESS	ممکن است کاربر دسترسی غیرمجازی به داده‌ها و کد اجرایی هدف ارزیابی پیدا کند. یک کاربر، پروسه مخرب یا موجودیت IT خارجی ممکن است خود را به عنوان موجودیت مجاز جا بزند تا بتواند به صورت غیرمجاز به داده‌ها یا منابع هدف ارزیابی دستیابی پیدا کند. یک کاربر، پروسه مخرب یا موجودیت IT خارجی ممکن است خودش را به عنوان هدف ارزیابی معرفی کند تا بتواند داده-های شناسایی و احراز هویت را به دست آورد.
T.UNAUTHORIZED_UPDATE	بخش مخرب سعی می‌کند به کاربر به روز رسانی از محصول ارائه دهد که ویژگی‌های امنیتی هدف ارزیابی را به خطر اندازد.
T.UNDETECTED_ACTIONS	کاربران مخرب از راه دور یا موجودیت‌های IT خارجی ممکن است اقدامی انجام دهند که امنیت هدف ارزیابی به صورت مخرب تحت تاثیر قرار بدهند. این اقدام ممکن است تشخیص داده نشده، باقی بماند و بنابراین نمی‌توان اثر اینگونه اقدامات را به طور موثری کاهش داد.
T.USER_DATA_REUSE	فرستنده ممکن است سهواً داده کاربری را به گیرنده‌ای ارسال کند که مدنظر نبوده است.
T.RESOURCE_EXHAUSTION	یک پروسه یا کاربر ممکن است دسترسی به خدمات هدف ارزیابی را با خارج کردن منابع حساس انکار کند.

۵,۲ خط‌مشی‌ها

P.TYPE	توضیحات
P.ACCESS_BANNER	هدف ارزیابی باید پرچم‌های اولیه‌ای را نمایش دهد که توصیف کننده محدودیت‌های استفاده، توافقات قانونی یا هرگونه اطلاعات مناسب دیگری است که کاربران با دستیابی به هدف ارزیابی با آنها موافقت می‌کنند.
P.COMPATIBILITY	هدف ارزیابی باید الزامات RFC ها را برای پروتکل‌های پیاده‌سازی شده در نظر بگیرد تا با استفاده از این پروتکل‌ها تقابل Wireless Client ها را با دیگر تجهیزات شبکه تسهیل کند.
P.ACCOUNTABILITY	کاربران مجاز هدف ارزیابی باید پاسخگوی اقداماتشان در هدف ارزیابی باشند.
P.ADMIN_ACCESS	سرپرستان هدف ارزیابی باید قادر به سرپرستی هدف ارزیابی (محلی و از راه دور) از طریق کانال‌های ارتباطی محافظت شده باشند.
P.EXTERNAL_SERVERS	هدف ارزیابی باید از پروتکل‌های استاندارد شده (RFC) برای ارتباط با یک سرور ممیزی مرکزی و سرور احرازهویت RADIUS پشتیبانی کند.

۵,۳ فرضیات

A.TYPE	توضیحات
A.PHYSICAL	امنیت فیزیکی متناسب با ارزش هدف ارزیابی و داده‌های مربوط به آن است و فرض می‌شود که امنیت فیزیکی توسط محیط فراهم می‌شود.
A.NO_GENERAL_PURPOSE	فرض می‌شود که قابلیت‌های محاسباتی همه‌منظوره (همانند کامپایلرها و برنامه های کاربردی کاربر) در دسترس هدف ارزیابی وجود ندارد مگر سرویس‌هایی که برای «کارکرد»، «سرپرستی» و «پشتیبانی» هدف ارزیابی لازم هستند.
A.TRUSTED_ADMIN	سرپرستان هدف ارزیابی جهت دنبال نمودن و به کاربردن مطمئن تمام راهنماهای سرپرستی، قابل اعتماد می‌باشند.
A.NO_TOE_BYPASS	اطلاعات نمی‌تواند بدون عبور از هدف ارزیابی بین wireless client ها و شبکه‌های داخلی جریان یابد.

۶ اهداف امنیتی

۶,۱ اهداف امنیتی هدف ارزیابی

O.TYPE	توضیحات
O.AUTH_COMM	هدف ارزیابی باید امکانی را فراهم کند تا اطمینان یابد که با «نقطه دسترسی مجاز» در ارتباط است و با «نقطه دسترسی» که تظاهر به مجاز بودن می‌کند در ارتباط نباشد، همچنین هدف ارزیابی باید نسبت به هویت خود به «نقطه دسترسی» اطمینان دهد.
O.VERIFIABLE_UPDATES	هدف ارزیابی قابلیتی را ارائه خواهد کرد تا اطمینان کند که بروزرسانی هدف ارزیابی توسط سرپرست تائید شده، بدون تغییر و از یک منبع قابل اطمینان است.
O.SYSTEM_MONITORING	هدف ارزیابی قابلیتی برای تولید داده‌های ممیزی و فرستادن این داده‌ها به یک موجودیت IT خارجی فراهم خواهد کرد.
O.CRYPTOGRAPHIC_FUNCTIONS	هدف ارزیابی باید عملکرد رمزنگاری داشته باشد تا بتواند محرمانگی را حفظ کند و امکان تشخیص تغییرات داده-ای را که به خارج از هدف ارزیابی و محیط میزبان منتقل می‌شود فراهم کند.
O.TOE_ADMINISTRATION	هدف ارزیابی سازوکارهایی ارائه خواهد داد تا اطمینان دهد که تنها سرپرستان قادر به وارد شدن به سامانه و پیکربندی هدف ارزیابی هستند و برای سرپرستان وارد شده به سامانه محافظتی فراهم خواهد کرد.
O.RESIDUAL_INFORMATION_CLEARING	هدف ارزیابی اطمینان خواهد داد هیچ یک از داده‌های یک منبع محافظت شده در زمان اختصاص دوباره آن منبع، در دسترس نیستند.
O.WIRELESS_CLIENT_ACCESS	هدف ارزیابی باید قادر به محدود نمودن نقاط دسترسی که به آن متصل خواهند شد، باشد.
O.TSF_SELF_TEST	هدف ارزیابی قابلیتی جهت آزمون برخی از زیر مجموعه عملکردهای امنیتی خود ارائه خواهد کرد تا از عملکرد مناسب آنها اطمینان حاصل کند.

O.DISPLAY_BANNER	هدف ارزیابی باید راجع به استفاده هدف ارزیابی، «پیغام مشورتی» به کاربران نمایش دهد.
O.FAIL_SECURE	هدف ارزیابی باید در ادامه شکست رخ داده، در وضعیت امنی قرار بگیرد.
O.PROTECTED_COMMUNICATIONS	هدف ارزیابی برای سرپرستان، دیگر بخش‌های هدف ارزیابی توزیع شده و موجودیت‌های IT مجاز، کانال‌های ارتباطی محافظت شده ارائه خواهد داد.
O.REPLAY_DETECTION	هدف ارزیابی این امکان را خواهد داد تا تکرار داده‌های احرازهویت و دیگر داده‌های توابع امنیتی هدف ارزیابی و مشخصه‌های امنیتی را تشخیص دهد و رد کند.
O.PROTOCOLS	هدف ارزیابی اطمینان خواهد داد که پروتکل‌های استاندارد شده در هدف ارزیابی براساس RFC و/یا مشخصه-های صنعتی پیاده‌سازی خواهند شد و قابلیت همکاری با قسمت‌های مختلف را خواهند داشت و همچنین از ارتباطات با سرور ممیزی مرکزی و سرور احرازهویت RADIUS پشتیبانی می‌کند.
O.RESOURCE_AVAILABILITY	هدف ارزیابی باید سازوکارهایی را بکار ببرد تا تلاش‌های کاربر را در بکارگیری و اتمام منابع هدف ارزیابی کاهش دهد(به طور مثال ذخیره‌سازی مداوم)
O.ROBUST_TOE_ACCESS	هدف ارزیابی باید سازوکارهایی ارائه دهد که کنترل کننده دسترسی منطقی سرپرست به هدف ارزیابی و دسترسی سرپرستی از یک wireless client باشد.
O.SESSION_LOCK	هدف ارزیابی سازوکارهایی ارائه خواهد داد که خطر سرقت[1] نشست‌های بدون مراقبت[2] را کاهش دهد.
O.TIME_STAMPS	هدف ارزیابی باید «مهرهای زمانی» معتبری ارائه دهد و به سرپرستان این امکان را بدهد تا زمان مورد استفاده برای این مهرهای زمانی را تنظیم کنند.

[1] Hijacked

[2] Unattended session

۶,۲ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
OE.NO_GENERAL_PURPOSE	به غیر از سرویس‌های لازم برای عملیات، سرپرستی و پشتیبانی هدف ارزیابی، هیچ قابلیت محاسباتی همه منظوره (همانند کامپایلرها یا برنامه‌های کاربردی) که بر روی هدف ارزیابی در دسترس باشند، وجود ندارد.
OE.NO_TOE_BYPASS	اطلاعات نمی‌تواند بین شبکه‌های داخلی و خارجی که در قلمروهای مختلفی قرار دارند، بدون عبور از هدف ارزیابی جریان یابد.
OE.PHYSICAL	امنیت فیزیکی متناسب با ارزش هدف ارزیابی و داده‌های آن، توسط محیط ارائه می‌شود.
OE.TRUSTED_ADMIN	سرپرستان هدف ارزیابی جهت دنبال نمودن و به کاربردن مطمئن تمام راهنماهای سرپرستی، قابل اعتماد می‌باشند.

۷ الزامات کارکرد امنیتی تجهیزات شبکه محلی بی‌سیم

در این بخش به بررسی حوزه‌ها، خانواده‌ها و الزامات امنیتی پرداخته شده است. استفاده از توابع، الگوریتم‌ها و ماژول‌های بومی که در مقایسه با معادل‌های استاندارد جهانی، به تایید نهادهای بالاسری مربوطه رسیده باشند، در اجرای عملیات ارزیابی امتیاز بالاتری خواهند داشت.

۷,۱ کلاس ممیزی امنیت

نام کلاس: ممیزی امنیت

شرح کلاس: تجهیزات شبکه بی‌سیم برای رخدادهای گوناگون اقدام به ایجاد گزارشهایی برای ممیزی می‌کنند. کلاس ممیزی امنیت، الزاماتی پیرامون نحوه شناخت، ثبت و ذخیره و آنالیز اطلاعات ممیزی مربوط به فعالیت‌های مرتبط امنیتی تعریف نموده است (فعالیت‌هایی که توسط توابع امنیتی هدف ارزیابی کنترل می‌شوند). با بررسی

ممیزی‌های ثبت شده می‌توان تعیین کرد کدام رخداد مرتبط با چه فعالیت امنیتی صورت گرفته و چه‌کسی (چه کاربری) مسوول آن است. این کلاس شامل ۵ خانواده است که عبارتند از:

- **خانواده پاسخ سامانه در برخورد با خطاهای امنیتی[1]**

این خانواده تعریف کننده الزامات برای واکنش‌های سامانه نسبت به رویدادهایی است که بروز آنها نشان‌دهنده نقض امنیتی بالقوه‌ای باشد.

- **خانواده تولید داده ممیزی[2]**

این خانواده الزاماتی را برای ثبت رخدادهای امنیتی مربوط به رویدادهایی که تحت کنترل توابع امنیتی هدف ارزیابی صورت می‌گیرند تعریف می‌کند. این خانواده سطح ممیزی را تعیین می‌کند، انواع رویدادهایی که بایستی توسط توابع امنیتی هدف ارزیابی قابل ممیزی باشند را بیان می‌کند و یک مجموعه حداقلی از اطلاعات مرتبط با ممیزی را تعیین می‌کند که باید در داخل انواع ممیزی‌های امنیتی ثبت شده، ارائه شوند.

- **خانواده تحلیل ممیزی امنیت[3]**

این خانواده الزاماتی برای ابزارهای خودکار، که فعالیت‌های سامانه را تحلیل می‌کند و داده‌های ممیزی را که نقص امنیتی واقعی یا ممکن را جستجو می‌کنند، تعریف می‌کند. این تحلیل ممکن است در پشتیبانی از تشخیص نفوذ، یا پاسخ خودکار به نقص امنیتی بالقوه کار کند.

1 Security audit automatic response (FAU_ARP)
2 Security audit data generation (FAU_GEN)
3 Security audit analysis (FAU_SAA)

- **خانواده بازبینی ممیزی امنیت[1]**

این خانواده تعریف کننده الزاماتی برای ابزارهای ممیزی است که باید در دسترس کاربران مجاز قرار بگیرند تا به بازبینی داده‌های ممیزی کمک کند.

- **خانواده انتخاب رویدادهای ممیزی امنیت[2]**

این خانواده تعریف کننده الزاماتی جهت انتخاب یک مجموعه رویدادهای ممیزی شده در طول عملکرد هدف ارزیابی، از بین تمام رویدادهای قابل ممیزی می‌باشد.

- **خانواده ذخیره‌سازی رویدادهای ممیزی امنیت[3]**

این خانواده تعریف کننده الزاماتی برای توابع امنیتی هدف ارزیابی است تا قادر به ایجاد و نگهداری از سوابق ممیزی بصورت امن باشند.

شماره الزام	نام خانواده	نام مؤلفه
۱	تولید داده ممیزی امنیت. **(FAU_GEN)**	**نام عنصر: تولید داده ممیزی امنیت ۱** **شماره مؤلفه: ما-ت‌ل.۱,۱ (FAU_GEN.1.1)** **شرح مؤلفه:**

1 Security audit review (FAU_SAR**)**

2 Security audit event selection (FAU_SEL)

3 Security audit event storage (FAU_STG)

توابع امنیتی هدف ارزیابی باید بتوانند از رویدادهای قابل ممیزی زیر یک رکورد ممیزی تولید کنند :

الف- آغاز و پایان عملیات ممیزی

ب- کلیه رویدادهای قابل ممیزی برای سطح ممیزی نامشخص

پ- همه فعالیت‌های سرپرستی

ت- [به طور مشخص رویدادهای قابل ممیزی تعریف و فهرست شده در جدول ۱]

الزامات	رویدادهای قابل ممیزی	محتویات رکوردهای ممیزی اضافی
م‌ا-ت‌ل.۱ **FAU_GEN.1**	هیچ	
م‌ا-ت‌ل.۲ **FAU_GEN.2**	هیچ	
م‌ا-اخ.۱ **FAU_SEL.1**	تمامی تغییرات پیکربندی ممیزی هنگامی رخ می‌دهد که عملکرد جمع‌آوری ممیزی انجام می‌گیرد.	هیچ
م‌ا-ذخ.۱ **FAU_STG.1**	هیچ	
م‌ا-ذخ.(ت‌س).۱ **FAU_STG_EXT.1**	هیچ	
م‌ا-ذخ.(ت‌س).۳ **FAU_STG_EXT.3**	هیچ	
رز-م‌ک.۱ (۱)	شکست فعالیت تولید کلید	هیچ

FCS_CKM.1(1)		
رز-م‌ک.۱(۲) **FCS_CKM.1(2)**	شکست فعالیت تولید کلید	هیچ
رز-م‌ک.۲ (۱) **FCS_CKM.2(1)**	شکست فعالیت توزیع کلید	هیچ
رز-م‌ک.۲ (۲) **FCS_CKM.2(2)**	شکست فعالیت توزیع کلید، هم‌چون شکست مربوط به پنهان نمودن GTK	شناسه(ها) برای درنظرگرفتن گیرنده‌های کلید پنهان شده
رز-م‌ک.(ت‌س).۴ **FCS_CKM_EXT.4**	شکست فرایند صفرسازی کلید	هویت موجودیت فعال تقاضا شده یا سبب صفر شدن است، هویت موجودیت غیرفعال یا موجودیت حذف شده
رز-ع‌ر.۱(۱) **FCS_COP.1(1)**	شکست رمزنگاری یا رمزگشایی	مود رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال رمز شده/رمزگشایی شده
رز-ع‌ر.۱(۲) **FCS_COP.1(2)**	شکست امضاء رمزنگاری	مود رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال امضاء شده/بررسی شده
رز-ع‌ر.۱(۳) **FCS_COP.1(3)**	شکست عملکرد درهم‌سازی	مود رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال درهم سازی شده
رز-ع‌ر.۱(۴) **FCS_COP.1(4)**	شکست در درهم‌سازی رمزنگاری برای صحت غیر داده[1]	مود رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال درهم سازی شده
رز-ع‌ر.۱(۵) **FCS_COP.1(5)**	شکست رمزنگاری یا رمزگشایی WPA2	مود رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال رمز شده/رمزگشایی شده، غیر هدف ارزیابی

1 Non-Data

		بودن نقطه پایانی اتصال (آدرس IP)
رز-IPSEC.(ت‌س).۱ **FCS_IPSEC_EXT.1**	پروتکل‌های شکست خورده برقراری/ اتمام IPSEC SA مذاکره «پائین» از تبادل IKEv2 به IKEv1	دلایل شکست نقطه پایانی اتصال غیر هدف ارزیابی (آدرس IP) برای موفقیت و شکست
اش-مع.(ت‌س).۱ **FIA_RBG_EXT.1**	شکست پروسه تصادفی	هیچ
اش-ش‌ه.(ت‌س).۱ **FDP_RIP.2**	هیچ	
اش-ش‌ا.۱ **FIA_AFL.1**	رسیدن به آستانه تلاش احراز هویت ناموفق و اقدامات صورت گرفته (به طور مثال غیرفعال نمودن حساب) و پس از آن، در صورت لزوم، به حالت نرمال برگرداندن (به عنوان مثال با دوباره فعال‌سازی ترمینال)	هیچ
اش- مع.(ت‌س).۱ **FIA_PMG_EXT.1**	هیچ	
اش-ش‌ه.(ت‌س).۱ **FIA_UIA_EXT.1**	تمام استفاده های سازوکار شناسایی و احراز هویت	ارائه دادن هویت کاربر، مبدا تلاش (به طور مثال آدرس IP)
اش-اه.۵ **FIA_UAU.5**	تمام استفاده‌های سازوکار احراز هویت	مبدا تلاش (به طور مثال آدرس IP)

اش-اه.۶ **FIA_UAU.6**	تلاش‌های دوباره احراز هویت	مبدا تلاش (به طور مثال آدرس IP)
اش-اه.۷ **FIA_UAU.7**	هیچ	
اش-8021X-(ت_س).۱ **FIA_8021X_EXT.1**	تلاش جهت دسترسی به پورت کنترل شده‌ی 802.1X	هویت کلاینت ارائه شده (آدرس IP)
اش-PSK-(ت_س).۱ **FIA_PSK_EXT.1**	هیچ	
اش-X509-(ت_س).۱ **FIA_X509_EXT.1**	تلاش جهت بارگذاری گواهینامه تلاش جهت ابطال گواهینامه	هیچ
مد-مت.۱ **FMT_MOF.1**	هیچ	
مد-مد.۱(۱) **FMT_MTD.1(1)**	هیچ	
مد-مد.۱(۲) **FMT_MTD.1(2)**	هیچ	
مد-مد.۱(۳) **FMT_MTD.1(3)**	هیچ	
مد-ع‌م.۱ **FMT_SMF.1**	هیچ	
مد-ع‌م.۱ **FMT_SMR.1**	هیچ	
حت-نا.۱ **FPT_FLS.1**	شکست توابع امنیتی هدف ارزیابی	نشان دادن توابع امنیتی هدف ارزیابی شکست خورده با نوع شکست رخ داده
حت-ش‌م.۱	تشخیص حمله‌ی تکرار	شناسایی کاربری که موجودیت فعال حمله‌ی تکرار

FPT_RPL.1		است. شناسایی (به طور مثال، آدرس IP مبدا) مبدا حمله-ی تکرار
ح‌ت-م‌ز.۱ **FPT_STM.1**	هیچ	
ح‌ت-رم.(ت‌س).۱ **FPT_TUD_EXT.1**	شروع به روزرسانی هرگونه شکستی در بررسی یکپارچگی و صحت به‌روزرسانی	بدون هیچ اطلاعات اضافه
ح‌ت-خا.(ت‌س).۱ **FPT_TST_EXT.1**	اجرای مجموعه خودآزمایی‌های توابع امنیتی هدف ارزیابی تشخیص نقض یکپارچگی	برای نقض یکپارچگی، فایل کد توابع امنیتی هدف ارزیابی که سبب نقض یکپارچگی شده است.
من-ت‌م.۱ **FRU_RSA.1**	فراتر بودن ازحداکتر ظرفیت	شناسه منبع
دس-ق‌ن.(ت‌س).۱ **FTA_SSL_EXT.1**	قفل نمودن نشست تعاملی توسط ساز و کار قفل نمودن نشست هر تلاشی که نشست تعاملی را بازگشایی کند	هیچ
دس-ق‌ن.۳ **FTA_SSL_EXT.3**	اتمام نشست راه دور توسط سازوکار قفل نمودن نشست	هیچ
دس-ق‌ن.۴ **FTA_SSL_EXT.4**	اتمام نشست با ترک آن یا خروج از آن	هیچ

دس‌ع‌د.۱ **FTA_TAB.1**	هیچ	
دس- ان.۱ **FTA_TSE.1**	انکار برقراری نشست با توجه به سازوکار برقراری نشست	دلیل انکار، مبدا تلاشی که برقرار شده است.
مم-ک‌م.۱ **FTP_ITC.1**	تمام تلاش برای برقراری یک کانال امن تشخیص تغییرات داده کانال	شناسایی آغازکننده و هدف از کانال
مم-ک‌م.۱ **FTP_TRP.1**	تمام تلاش‌هایی که جهت برقراری یک نشست سرپرستی راه دور انجام می‌گیرد. تشخیص تغییرات داده نشست	شناسایی آغازگر موجودیت IT (به طور مثال، آدرس IP)

جدول ۱: الزامات عملکرد امنیتی هدف ارزیابی

نکته کاربردی:

نویسنده هدف امنیتی می‌تواند اعلام کند که هدف ارزیابی قادر به تولید سایر رویدادهای قابل ممیزی نیز می باشد و آنها را لیست کند و لیست رویدادهای قابل ممیزی، محدود به فهرست ارائه شده نیست.

بسیاری از جنبه‌های قابل ممیزی الزامات عملکردهای امنیتی که در این سند آورده شده است مرتبط با فعالیت‌های سرپرستی هستند.آیتم پ بالا الزام می‌دارد که همه فعالیت‌های سرپرستی قابل ممیزی باشد، بنابراین هیچ ویژگی اضافی از این فعالیت‌های قابل ممیزی در جدول ۱ مشخص نشده است.

۲ **نام عنصر: تولید داده ممیزی امنیتی ۱**

شماره مؤلفه: ما-ت‌ل.۲,۱(FAU_GEN.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید در هر رکورد ممیزی، حداقل اطلاعات زیر را ثبت کند:

الف - تاریخ و زمان رویداد، نوع رویداد، هویت موجودیت فعال و نتیجه (موفقیت یا شکست) رویداد

ب- برای هر نوع رویداد ممیزی، بر اساس تعریفهای رویداد قابل ممیزی عناصر عملیاتی موجود در پروفایل حفاظتی/هدف امنیتی.[اطلاعات مشخص شده در ستون ۳ جدول ۱ آمده است]

نکته کاربردی:

همچون مؤلفه قبلی، نویسنده هدف امنیتی می‌تواند جدول ۱ بالا را با هر نوع اطلاعات تولید شده به‌روزرسانی کند. برای مثال « هویت موجودیت فعال » در متن این الزام می‌تواند شناسه کاربر سرپرست یا واسط شبکه مورد نظر باشد.

۳ **نام عنصر: انجمن ممیزی کاربر ۲**

شماره مؤلفه: ما-ت‌ل.۲,۱(FAU_GEN.1.2)

شرح مؤلفه:

برای رویدادهای ممیزی ناشی از اقدامات کاربران شناسایی شده، توابع امنیتی هدف ارزیابی باید قادر به مرتبط کردن هر رویداد قابل ممیزی به هویت کاربری که سبب رویداد شده است، باشد.

نکته کاربردی:

برای تلاش‌های ورودی که منجر به شکست شده است، در جایی که شناسه کاربری مطابق شناسه کاربر شناخته شده نیست، لزومی ندارد که کاربر مرتبط شود زیرا کاربر تا زمانی‌که به صورت موفقی شناسایی/احراز هویت نشود تحت کنترل توابع امنیتی هدف ارزیابی نیست.

۴ **نام عنصر: ممیزی انتخابی ۱**

شماره مؤلفه: م‌ا-اخ.۱،۱(FAU_SEL.1.1)

شرح مؤلفه:

انتخاب رویداد ممیزی امنیت **(FAU_SEL)**

توابع امنیتی هدف ارزیابی باید قابلیت انتخاب رویدادهای قابل ممیزی را بر اساس دارا بودن/ نبودن ویژگی‌های زیر از مجموعه رویدادهای ممیزی داشته باشد :

الف- نوع رویداد

ب-هویت سرپرست

پ-موفق بودن رویداد امنیتی قابل ممیزی

ت-شکست رویداد امنیتی قابل ممیزی

ث- [اختصاص: دیگر ویژگی‌ها].

نکته کاربردی:

منظور این الزام آن است که تمام معیارهایی را که می‌توانند جهت راه‌اندازی رویدادهای ممیزی انتخاب شوند معرفی کند. برای نویسنده هدف امنیتی، از قسمت «اختصاص» کمک گرفته شده است، تا بتواند معیارهای بیشتری را لیست کند یا «هیچکدام» را برگزیند. انواع رویدادهای قابل ممیزی در جدول ۱ لیست شده است.

۵ **نام عنصر: ذخیره‌سازی دنباله ممیزی محافظت شده(ذخیره محلی) ۱**

شماره مؤلفه: م‌ا-ذخ.۱،۱(FAU_STG.1.1)

شرح مؤلفه:

ذخیره‌سازی رویدادهای ممیزی امنیتی **(FAU_STG)**

توابع امنیتی هدف ارزیابی باید [اختصاص: مقدار ذخیره‌سازی] رکوردهای ممیزی ذخیره شده دردنباله ممیزی را از حذف غیرمجاز محافظت کند.

۶ **نام عنصر: ذخیره‌سازی دنباله ممیزی محافظت شده(ذخیره محلی) ۱**

شماره مؤلفه: م‌ا-ذخ.۱،۲(FAU_STG.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر باشد تا از تغییرات غیرمجاز رکوردهای ممیزی ذخیره شده در دنباله ممیزی جلوگیری کند.

نکته کاربردی:

علاوه بر قابلیت صدور اطلاعات ممیزی، هدف ارزیابی نیاز به مقداری حافظه محلی دارد. نویسنده هدف امنیتی قسمت «اختصاص» را با مقداری ذخیره‌سازی محلی در دسترس برای رکوردهای ممیزی تکمیل می‌کند، مقدار متوسط رکوردهای ممیزی می‌تواند در حد مگابایت باشد.

نام عنصر: ذخیره‌سازی دنباله ممیزی خارجی ۱ ۷

شماره مؤلفه: ما-ذخ.(ت‌س).۱,۱(FAU_STG_EXT.1.1))

شرح مؤلفه :

توابع امنیتی هدف ارزیابی باید قادر باشد داده ممیزی تولید شده را با استفاده از کانال امنی که توسط پروتکل‌های [انتخاب: IPsec، SSH، TLS، TLS/HTTPS] پیاده‌سازی شده‌اند، به موجودیت IT خارجی منتقل کند.

نکته کاربردی:

هدف امنیتی، به سرور ممیزی غیرهدف امنیتی برای ذخیره و بازبینی رکوردهای ممیزی متکی است. هرچند هدف امنیتی رکوردهای ممیزی تولید می‌کند، ذخیره این رکوردهای ممیزی و توانایی سرپرست در بازبینی این رکوردهای ممیزی توسط محیط عملیاتی فراهم می‌شود. نویسنده هدف امنیتی در قسمت انتخاب، باید پروتکلی را انتخاب کند تا اتصال توسط آن محافظت شود. نویسنده هدف امنیتی

اطمینان می‌دهد که الزامات پروتکل پشتیبانی مطابق انتخاب در برگرفته شده در هدف امنیتی است.

۸ **نام عنصر: عملکرد در زمان ازدست رفتن اتصال سرور ممیزی ۳**

شماره مؤلفه: ما-ذخ.(ت‌س).۱,۳(FAU_STG_EXT.3.1)

شرح مؤلفه :

توابع امنیتی هدف ارزیابی باید [اختصاص: اقدام] اگر اتصال به موجودیت خارجی جمع‌آوری کننده داده ممیزی تولید شده توسط هدف امنیتی باشد که در دسترس نمی‌باشد.

نکته کاربردی:

اگر اتصال به سرور ممیزی غیرقابل دسترس باشد، نویسنده هدف امنیتی قسمت «اختصاص» را با اقدامی که هدف امنیتی صورت می-دهد(متوقف نمودن صدور بسته و ...)، تکمیل می‌کند.

۷,۲ کلاس پشتیبانی از رمزنگاری

نام کلاس: پشتیبانی از رمزنگاری

شرح کلاس: توابع امنیتی هدف ارزیابی ممکن است با به کار بردن قابلیت‌های رمزنگاری، به برآورده شدن چندین هدف امنیتی سطح بالا کمک کنند: این اهداف می‌توانند شامل موارد زیر باشند، اما تنها به این دسته نیز محدود نمی‌شوند:

- شناسایی و احراز هویت
- عدم انکار
- مسیر امن
- کانال امن
- مجزاسازی داده

این کلاس زمانی‌که هدف ارزیابی، عملکرد رمزنگاری را پیاده‌سازی می کند، استفاده می‌شود این پیاده‌سازی می‌تواند در نرم‌افزار، سخت‌افزار و میان افزار صورت گیرد.

- **خانواده مدیریت کلید رمزنگاری[۱]**

کلیدهای رمزنگاری باید از طریق دوره حیاتشان مدیریت شوند. این خانواده برای پشتیانی از دوره حیات کلید در نظر گرفته می‌شود و درنتیجه الزاماتی را برای فعالیت‌های زیر تعریف می کند:

- تولید کلید رمزنگاری
- توزیع کلید رمزنگاری
- دستیابی به کلید رمزنگاری
- تخریب کلید رمزنگاری

در صورت وجود الزامات عملیاتی برای مدیریت کلیدهای رمزنگاری، این خانواده نیز باید در نظر گرفته شود.

- **خانواده عملیات رمزنگاری [۱]**

[۱] Cryptographic key management(FCS_CKM)

به منظور عملکرد صحیح عملیات رمزنگاری، این عملیات باید مطابق با الگوریتم خاص و کلید رمزنگاری با اندازه مشخص انجام گیرد. در صورت وجود الزامات عملیاتی برای مدیریت کلیدهای رمزنگاری، این خانواده نیز باید در نظر گرفته شود.

معمولاً عملیات رمزنگاری شامل رمزنگاری و رمزگشایی داده، تائید و/یا تولید امضای دیجیتال، تولید کنترل [۲]رمزنگاری برای یکپارچگی و صحت و یا تائید کنترل، درهم-سازی امن (خلاصه پیام)، رمزنگاری و/یا رمزگشایی کلید رمزنگاری و توافق کلید رمزنگاری می‌باشد.

شماره الزام	نام خانواده	عنصر امنیتی
۹	تولید کلید رمزنگاری **(FCS_CKM)**	**نام عنصر: مدیریت کلید رمزنگاری (کلیدهای متقارن برای اتصالات WPA2) ۱ (۱)** **شماره مؤلفه: رز-م‌ک.۱،۱(۱) ((FCS_CKM.1.1(1))** **شرح مؤلفه :** توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری متقارن مطابق با الگوریتم استخراج کلید رمزنگاری مشخص شده[PRF-384]، با اندازه کلید رمزنگاری[۱۲۸ بیت] با استفاده از تولیدکننده بیت تصادفی RBG مشخص شده در الزام رز-ب‌ت.(ت‌س).۱ و با زمان ارسال و دریافت تنظیم شده توسط سرپرست که استاندارد [802.11-2007] را برآورده می‌کند، استخراج کند.

[۱] Cryptographic operation(FCS_COP)

[۲] checksum

شماره الزام	نام خانواده عنصر امنیتی

نکته کاربردی :

این الزام، تنها کلیدهایی را به کار می‌برد که برای ارتباط بین نقطه دسترسی و کلاینت، زمانی‌که کلاینت احراز هویت شده است تولید و استخراج می‌شود. این الزام اشاره به استخراج PTK از PMK دارد، که با استفاده از یک مقدار تصادفی توسط RBG مشخص شده در این پروفایل حفاظتی ، تابع HMAC با استفاده از الگوریتم SHA-1 مشخص شده در این پروفایل حفاظتی و هم‌چنین اطلاعات تولید می‌شود. این مساله در استاندارد 802.11-2007 فصل هشتم مشخص شده است.

۱۰ **نام عنصر: توزیع کلید رمزنگاری(کلیدهای نامتقارن) ۱ (۲)**

شماره مؤلفه: رز-م‌ک. ۱,۱ (۲) ((FCS_CKM.1.1(2))

شرح مؤلفه :

توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری نامتقارن مورد استفاده برای ایجاد کلید را مطابق با انتخاب‌های زیر تولید کند.

[انتخاب:

- استاندارد NIST SP 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته» برای طرح برقراری کلید متناهی مبتنی بر میدان[1]

1 Field-bsae

شماره الزام	نام خانواده عنصر امنیتی

- استاندارد NIST 800-56 A، «توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری لگاریتمی گسسته[1]» برای برقراری طرح کلید مبتنی بر بیضوی منحنی[2] و پیاده‌سازی «NIST Curves» در P-256 و P-384 و [انتخاب: P-521، و نه منحنی دیگری] (چنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده است)
- استاندارد NIST SP 800-56 B، " توصیه برای طرح برقراری جفت کلید با استفاده از رمزنگاری تجزیه عدد صحیح[3] برای طرح برقراری کلید مبتنی بر RSA.]

و اندازه‌های کلید رمزنگاری شده معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی

نکته کاربردی:

این مؤلفه الزام می‌دارد که هدف ارزیابی قادر به تولید جفت کلید عمومی/خصوصی باشد که برای اهداف ایجاد کلید به منظور پروتکل-های مختلف رمزنگاری استفاده شده توسط هدف ارزیابی (برای مثال، IPsec) استفاده می شوند. اگر طرح‌های چندگانه پشتیبانی شوند، نویسنده هدف امنیتی باید این الزام را برای بیان کردن این قابلیت‌ها تکرار کند. طرح مورد استفاده از انتخاب‌های گفته شده توسط نویسنده هدف امنیتی برگزیده خواهد شد.

از آنجا که پارامترهای دامنه که باید استفاده شوند توسط الزامات پروتکل در این پروفایل حفاظتی مشخص شده‌اند، انتظار نمی‌رود که

1 Discrete Logarithm Cryptography

2 Curve-base

3 Integer Factorization Cryptography

شماره الزام	نام خانواده عنصر امنیتی
	هدف ارزیابی پارامترهای دامنه را تولید کند و بنابراین به اعتبار سنجی اضافی پارامترهای دامنه وقتی‌که هدف ارزیابی با پروتکل‌های تعریف شده در این پروفایل حفاظتی مطابقت دارد، نیازی نیست. قدرت کلید تولید شده ۲۰۴۸ بیتی DSA و rDSA معادل یا بزرگتر از قدرت یک کلید متقارن ۱۱۲ بیتی است. استاندارد NIST 800-57(«توصیه برای مدیریت کلید» در خصوص قدرت کلید معادل) را ببینید.
۱۱	**نام عنصر: توزیع کلید رمزنگاری(کلیدهای نامتقارن) ۲ (۱)** **شماره مؤلفه: رز-م‌ک. ۱,۲ (۱) ((FCS_CKM.2.1(1))** **شرح مؤلفه :** توابع امنیتی هدف ارزیابی، باید جفت کلید اصلی 802.11 مطابق با روش توزیع کلید رمزنگاری مشخص: [دریافت از سرور احرازهویت 802.1X] که استاندارد [802.11-2007] برآورده می کند، توزیع کند و کلیدهای رمزنگاری را افشاء نکند. **نکته کاربردی:** این الزام به جفت کلید اصلی که از سرور RADIUS تویط هدف ارزیابی در یافت شده است، اعمال می‌شود. منظور این الزام اطمینان

شماره الزام	نام خانواده عنصر امنیتی

یافتن از پیاده‌سازی احراز هویت 802.1X توسط هدف‌های ارزیابی مطابق با این پروفایل حفاظتی پیش از برقراری ارتباط امن با کلاینت می‌باشد، علاوه بر این پیاده‌سازی‌هایی که تنها از کلیدهای از پیش به اشتراک گذارده شده، استفاده می کنند پذیرفته نمی‌شوند. زیرا لازم است ارتباط با سرور RADIUS بر روی اتصال محافظت شده IPsec انجام شود تا جفت کلید اصلی (PMK) محافظت شده منتقل شود.

۱۲ **نام عنصر: توزیع کلید رمزنگاری(GTK) ۲ (۲)**

شماره مؤلفه: رز-م‌ک. ۱,۲ (۲) ((FCS_CKM.2.1(2))

شرح مؤلفه :

توابع امنیتی هدف ارزیابی، باید کلید موقتی گروهی (GTK) را مطابق با روش توزیع کلید رمزنگاری مشخص: [پنهان نمودن کلید AES در یک قالب کلید EAPOL] که استاندارد [RFC 3394 برای پنهان نمودن کلید AES، 802.11-2007 برای قالب بسته و زمان‌بندی درنظرگرفته شده] برآورده می کند، توزیع کند و کلیدهای رمزنگاری را افشاء نکند.

نکته کاربردی:

این الزام به کلیدهای موقتی گروهی (GTK) که توسط هدف ارزیابی تولید شده است برای آنکه از این کلیدها در پیغام‌های چند بخشی

شماره	نام خانواده
الزام	عنصر امنیتی

و پخشی به کلاینت‌های متصل شده به هدف ارزیابی، استفاده شوند. استاندارد 802.11-2007 قالبی را برای انتقال مشخص می‌کند هم-چنین کلید باید توسط روش پنهان نمودن کلید AES مشخص شده در RFC 3394 پنهان شود.

۱۳

نام عنصر: صفرسازی کلید رمزنگاری ۴

شماره مؤلفه: رز-م‌ک-(ت‌س).۱,۴ (FCS_CKM.4.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید تمام کلیدهای رمزنگاری خصوصی و مخفی و پارامترهای بحرانی امنیتی رمزنگاری (CSP) را که دیگر مورد استفاده قرار نمی‌گیرند، صفر کند.

نکته کاربردی:

هرگونه اطلاعات مرتبط امنیتی (هم‌چون کلید، داده احراز هویت و رمز عبور) باید زمانی‌که مورد استفاده قرار نمی‌گیرد، صفر شود تا از فاش شدن و تغییر داده‌های حساس امنیتی جلوگیری کند.

شماره الزام	نام خانواده	عنصر امنیتی
۱۴	عملیات رمزنگاری (FCS_COP)	عمل صفرسازی کلید که در این الزام به آن اشاره شده است، به هر فضای ذخیره‌سازی واسط برای کلیدهای مخفی و پارامترهای امنیتی رمزنگاری (CSP) اعمال می‌شود به محض آنکه از کلید/CSP به موقعیت دیگر منتقل می‌شود. **نام عنصر: عملیات رمزنگاری(برای رمزنگاری/رمزگشایی داده) ۱ (۱)** **شماره مؤلفه: رز-ع‌ر.۱٫۱ (۱)((FCS_COP.1.1(1))** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید [کدبندی و کدگشایی] را مطابق با الگوریتم رمزنگاری مشخص شده [AES که در[اختصاص: یک یا بیش از یک مود]] عمل می‌کند و اندازه‌های کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی و [انتخاب : ۱۹۲ بیتی ، نه هیچ اندازه دیگری] که با موارد زیر تطابق داشته باشد انجام دهد : • استاندارد FIPS PUB 197، "AES" • [انتخاب:NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, , NIST SP 800-38D , NIST SP 800-38E] **نکته کاربردی:** در قسمت «اختصاص»، نویسنده هدف امنیتی باید مود یا مودهایی را که در آن مودها AES عمل می‌کند را انتخاب کند. برای انتخاب اول، نویسنده هدف امنیتی باید اندازه کلیدی را که توسط این عملکرد پشتیبانی می‌شود، انتخاب کند. برای انتخاب دوم، نویسنده هدف

شماره الزام	نام خانواده

عنصر امنیتی

امنیتی باید استانداردهایی را انتخاب کند که مودهای مشخص شده در قسمت «اختصاص» را توصیف می‌کنند.

قابل ذکر است که این الزام به رمزنگاری ترافیک بدون سیم اعمال نمی‌شود. الزام رز-ع‌ر.۱(۵) مود، اندازه کلید و استانداردهایی را تعریف می‌کند که برای رمزنگاری/رمزگشایی WPA2 بدون سیم استفاده می‌شود.

۱۵ **نام عنصر: عملیات رمزنگاری(برای امضای دیجیتال) ۱ (۲)**

شماره مؤلفه: رز-ع‌ر.۱،۱ (۲)((FCS_COP.1.1(2))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید خدمات رمزنگاری امضا را مطابق با موارد زیر انجام دهند:

[انتخاب :

- الگوریتم امضای دیجیتال (DSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با FIPS PUB 186-3، «استاندارد امضای دیجیتال»
- الگوریتم امضای دیجیتال RSA (rDSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با FIPS PUB 186-3، «استاندارد امضای دیجیتال»
- الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA[1]) با کلید ۲۵۶ بیتی یا بیشتر مطابق با
  - [انتخاب: FIPS PUB 186-3، «استاندارد امضای دیجیتال»]
  - تابع ارزیابی امنیتی باید منحنی‌های استاندارد « NIST curves »، P-256، P384 و [انتخاب : P251 ، نه سایر منحنی‌ها] (هم‌چنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده‌است)].

1 Elliptic Curve Digital Signature Algorithm

شماره	نام خانواده	عنصر امنیتی
الزام		

نکته کاربردی:

نویسنده هدف امنیتی باید الگوریتمی را برای امضاء دیجیتال انتخاب کند؛ اگر بیش از یک الگوریتم در دسترس باشد، این الزام باید تکرار شود تا عملکرد مشخص شود. برای الگوریتم انتخاب شده، نویسنده هدف امنیتی باید انتخاب/اختصاص مناسبی برای مشخص کردن پارامترهایی که برای آن الگوریتم پیاده‌سازی شده‌اند داشته باشد.

۱۶ **نام عنصر:** عملیات رمزنگاری(درهم‌سازی رمزنگاری) **۱ (۳)**

شماره مؤلفه: رز-ع‌ر.۱,۱ (۳)(FCS_COP.1.1(3))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [خدمات درهم‌سازی رمزنگاری] را مطابق با یک الگوریتم رمزنگاری مشخص [انتخاب: *SHA-1 SHA-256, SHA-384,*] و اندازه‌های خلاصه پیام[1][انتخاب: ۱۶۰، ۲۵۶ و ۳۸۴ بیت] که مطابق با FIPS 180-3، «استاندارد درهم‌ساز امن» باشد، انجام دهد.

نکته کاربردی:

انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد، به طور مثال اگر SHA-1 انتخاب شده است، تنها انتخاب، اندازه

1 Message Digest Sizes

شماره الزام	نام خانواده	عنصر امنیتی

خلاصه پیام قابل قبول ۱۶۰ بیت خواهد بود.

۱۷ **نام عنصر: عملیات رمزنگاری** (کد احراز هویت پیام مبتنی بر درهمسازی-کلید) **۱(۴)**

شماره مؤلفه: رز-ع‌ر.۱,۱(۴) ((FCS_COP.1.1(4))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [کد احراز هویت پیام مبتنی بر درهم‌سازی-کلید] را در تطابق با یک الگوریتم رمزنگاری مشخصHMAC -[انتخاب:SHA-1, SHA-256, SHA-384]، با اندازه کلید [اختصاص : اندازه کلید (بیت) استفاده شده در HMAC]، و اندازه‌های خلاصه پیام [انتخاب: ۱۶۰، ۲۵۶و ۳۸۴ بیت] که مطابق با FIPS 198-1، «کد احراز هویت پیام مبتنی بر درهمسازی-کلید» و FIPS 180-3، «استاندارد درهم‌ساز امن» باشد، انجام دهد.

نکته کاربردی:

انتخاب الگوریتم درهم‌سازی باید متناسب با اندازه خلاصه پیام باشد، به طور مثال اگر HMAC-SHA-256 انتخاب شده است، تنها انتخاب، اندازه خلاصه پیام قابل قبول ۲۵۶ بیت خواهد بود.

اندازه خلاصه پیام‌های بالا متناسب با الگوریتم درهم‌سازی مورد استفاده می‌باشد. کوتاه شدن خروجی HMAC پس از محاسبه درهم-

شماره الزام	نام خانواده	عنصر امنیتی

سازی یک گام مناسب در یک طیفی از برنامه‌های کاربردی است. کوتاه شدن پیام، اندازه خروجی نهایی و استانداردی که پیام کوتاه شده منطبق برآن است باید در هدف امنیتی بیان شود.

۱۸ **نام عنصر: عملیات رمزنگاری(رمزنگاری/رمزگشایی داده WPA2) ۱(۵)**

شماره مؤلفه: رز-ع‌ر.۱,۱(۵) ((FCS_COP.1.1(5))

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید رمزنگاری و رمزگشایی را در تطابق با یک الگوریتم رمزنگاری مشخص AES CCMP و اندازه کلید ۱۲۸ بیتی که مطابق با FIPS PUB 197، NIST SP 800-38C و IEEE 802.11-2007 انجام دهد.

نکته کاربردی:

توجه شود که باید انطباق با استاندارد IEEE 802.11-2007، AES CCMP با اندازه کلید رمزنگاری ۱۲۸ بیت پیاده‌سازی شود. در آینده این استاندارد به روزرسانی خواهد شد و مودهای رمزنگاری جدید بازبینی می‌شود و توسط NIST تصویب می‌شود، این الزام ممکن است شامل الزاماتی برای مودهای رمزنگاری جدید/اضافی و اندازه کلید باشد.

۱۹ پروتکل IPsec **نام عنصر: پروتکلIPsec ۱**

شماره الزام	نام خانواده	عنصر امنیتی
(FCS_IPSEC_EX (T		**شماره مؤلفه: رز-اپ-(ت‌س).۱٫۱ (FCS_IPSEC_EXT.1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید معماری Ipsec با پروتکل ESP به صورت مشخص شده در RFC 4301 با استفاده از الگوریتم‌های رمزنگاری AES-CBC-128، AES-CBC-256 (هردوی این الگوریتم‌ها در RFC 3602 مشخص شده است)، [انتخاب: هیچ الگوریتم دیگر، AES-GCM-128، AES-GCM-256 به صورت مشخص شده در RFC 4106]، و با استفاده از [انتخاب:

IKEv1 به صورت تعریف شده در RFC 2407، 2408، 2409، RFC 4109، و [انتخاب: هیچ RFC برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی]؛

IKEv2 به صورت تعریف شده در RFC 5996، 4307، و [انتخاب: هیچ RFC برای توابع درهم‌سازی، RFC 4868 برای توابع درهم‌سازی]] برای متصل نمودن سرور احراز هویت و [انتخاب: هیچ سرور دیگر، [اختصاص: لیستی از سرورهایی که به هدف ارزیابی متصل می‌شوند]]

را پیاده‌سازی کنند.

۲۰ **نام عنصر: پروتکلIPsec ۱**

شماره	نام خانواده	عنصر امنیتی
الزام		
		شماره مؤلفه: رز-اپ-(ت‌س).۲,۱.۱ (FCS_IPSEC_EXT.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید اطمینان بدهند که تنها محرمانگی ESP و سرویس‌های امنیتی یکپارچه استفاده می‌شود.
۲۱		**نام عنصر: پروتکلIPsec ۱**
		شماره مؤلفه: رز-اپ-(ت‌س).۳,۱.۱ (FCS_IPSEC_EXT.1.3)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید اطمینان دهند که تبادلات فاز ۱ IKEv1، تنها از مود اصلی استفاده می کنند.
۲۲		**نام عنصر: پروتکلIPsec ۱**
		شماره مؤلفه: رز-اپ-(ت‌س).۴,۱.۱ (FCS_IPSEC_EXT.1.4)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید اطمینان دهند که [انتخاب: محدود نمودن طول عمر ارتباط یک طرفه(SA) IKEv1 توسط تعداد بسته و زمان: ۲۴ ساعت برای فاز ۱ SA و ۸ساعت برای فاز ۲ SA؛ طول عمر ارتباط یک طرفه(SA) IKEv2 توسط سرپرست براساس تعداد

شماره الزام	نام خانواده عنصر امنیتی

بسته یا بازه زمانی پیکربندی شود.]

نکته کاربردی:

نویسنده هدف امنیتی با توجه به انتخابی که در اولین الزام داشته است، الزاماتی را برای پروتکل IKEv1 یا الزاماتی را برای پروتکل IKEv2 یا هر دو انتخاب می کند. الزامات پروتکل IKEv1 می‌تواند با ارائه طول عمر قابل تنظیم توسط سرپرست مجاز (با دستورالعمل-های مناسب در سندهای نگهداری شده توسط AGD_OPE) صورت بگیرد یا توسط «کدنویسی سخت»در این پیاده‌سازی محدود شود. برای پروتکل IKEv2، هیچ کدنویسی سخت محدود شده وجود ندارد، اما در این مورد لازم است که سرپرست قادر به تنظیم مقادیر باشد. به طور کلی، دستورالعمل‌ها برای تنظیم پارامترهای پیاده‌سازی، شامل طول عمر SA بایستی در سند راهنمای تولید شده برای AGD_OPE در نظرگرفته شده باشد.

تا زمانی‌که هدف ارزیابی قادر است محدودیتی بر روی میزان ترافیکی که توسط آن کلید محافظت شده است، درنظر بگیرد، تصحیح الزام به صورت تعداد MB/KB به‌جای تعداد بسته، مناسب می‌باشد (کل ظرفیت ترافیک پروتکل IPsec توسط آن کلید محافظت می‌شود).

۲۳	**نام عنصر: پروتکل IPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۵,۱ (FCS_IPSEC_EXT.1.5)

شماره **نام خانواده**

الزام

عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید مقدار x را با استفاده از تولید کننده بیت تصادفی (RBG) مشخص شده در الزام رز-بت.(ت‌س).۱ تولید کند که در تبادل کلید دیفی-هلمن (x در g^x mod p) استفاده می‌شود. و دارای حداقل اندازه [اختصاص: (یک یا بیش از) تعداد بیت حداقل دو برابر مقدار «بیت امنیتی» مربوط به گروه دیفی-هلمن لیست شده در جدول ۲ استاندارد ,NIST SP 800-57 «توصیه برای مدیریت کلید-بخش ۱: کلیت»] بیت باشد.

نکته کاربردی:

از آنجاکه پیاده‌سازی ممکن است به گروه‌های دیفی-هلمن مختلف اجازه بدهند تا برای استفاده در تشکیل SA ها مذاکره شوند. اختصاص‌ها در الزام‌های «رز-اپ-(ت‌س).۶,۱» و «رز-اپ-(ت‌س).۵,۱» ممکن است شامل مقادیر مختلف باشد. برای هر گروه DH پشتیبانی شده، نویسنده هدف امنیتی از جدول ۲ در استاندارد 57-800 برای تعیین «بیت امنیتی» مربوط به گروه DH کمک می‌گیرد. هر مقداری که منحصر به فرد است در تکمیل قسمت اختصاص استفاده می‌شود (در الزام ۱,۵ آنها دوبرابر می‌شوند؛ و در الزام ۱,۶ مستقیماً در قسمت اختصاص اضافه می‌شوند). برای مثال، فرض شود که پیاده‌سازی از گروه ۱۴ DH (2048 بیت MODP) و گروه ۲۰ (ECDH با استفاده از منحنی NIST P-384) پشتیبانی می کنند. توسط جدول ۲، بیت «مقدار امنیتی» برای گروه ۱۴، ۱۱۲ می‌باشد و

شماره الزام	نام خانواده عنصر امنیتی

برای گروه ۲۰، ۱۹۲ می‌باشد. بنابراین قسمت اختصاص برای الزام رز-اپ-(ت‌س).۵,۱ به صورت "[224,384]" و برای رز-اپ-(ت-س).۶,۱ به صورت "[112,192]" می‌باشد.

۲۴ **نام عنصر: پروتکلIPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۶,۱ (FCS_IPSEC_EXT.1.6)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید عدد تصادفی(nonce) را تولید کنند که در تبادلات IKE استفاده می‌شود به طوری‌که احتمال تکرار این عدد در دوره حیات SA مربوط به پروتکل IPsec کمتر از ۱ در ۲^ [اختصاص: (یک یا بیش از یک) مقدار «بیت‌های امنیتی» مربوط به گروه مذاکره Diffie-Hellman (که در جدول ۲ از NIST SP 800-57 لیست شده است، پیشنهادی برای مدیریت کلید- بخش ۱: کلیات) باشد] است.

نکته کاربردی:

از آنجاکه پیاده‌سازی ممکن است به گروه‌های دیفی-هلمن مختلف اجازه بدهند تا برای استفاده در تشکیل SA ها مذاکره شوند. اختصاص‌ها درالزام‌های «رز-اپ-(ت‌س).۶,۱» و«رز-اپ-(ت‌س).۵,۱» ممکن است شامل مقادیر مختلف باشد. برای هر گروه DH

شماره الزام	نام خانواده عنصر امنیتی

پشتیبانی شده، نویسنده هدف امنیتی از جدول ۲ در استاندارد 57-800 برای تعیین «بیت امنیتی» مربوط به گروه DH کمک می‌گیرد. هر مقداری که منحصر به فرد است در تکمیل قسمت اختصاص استفاده می‌شود (برای ۱,۵ آنها دوبرابر می‌شوند؛ برای ۱,۶ مستقیماً در قسمت اختصاص اضافه می‌شوند). برای مثال، فرض شود که پیاده‌سازی از گروه ۱۴ DH (2048 بیت MODP) و گروه ۲۰ (ECDH با استفاده از منحنی NIST P-384) پشتیبانی می کنند. توسط جدول ۲، بیت «مقدار امنیتی» برای گروه ۱۴، ۱۱۲ می‌باشد و برای گروه ۲۰، ۱۹۲ می‌باشد. بنابراین قسمت اختصاص برای الزام «رز-اپ-(ت‌س).۵,۱» به صورت "[224,384]" و برای الزام «رز-اپ-(ت‌س).۶,۱» به صورت "[112,192]" می‌باشد.

۲۵

نام عنصر: پروتکلIPsec ۱

شماره مؤلفه: رز-اپ-(ت‌س).۷,۱ (FCS_IPSEC_EXT.1.7)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تمام پروتکل‌های IKE گروه‌های Diffie-Hellman ۱۴(2048-bit MODP)، ۱۹ (256-bit MODP) و [انتخاب: ۵ (1536-bit MODP)، ۲۴ (2048-bit MODP با 256-bit POS)، ۲۰ (384-bit Random ECP)، [اختصاص:

شماره الزام	نام خانواده عنصر امنیتی

دیگر گروه‌های DH که توسط هدف ارزیابی پیاده‌سازی شده‌اند]، هیچ گروه DH دیگر] را پیاده‌سازی می‌کنند.

نکته کاربردی:

از قسمت «انتخاب» در این الزام برای مشخص نمودن گروه‌های DH اضافی که پشتیبانی شده‌اند، استفاده می‌شود. در نسخه‌های بعدی این پروفایل حفاظتی،به گروه DH 19 (256 بیت تصادفی ECP) و گروه DH 20 (384 بیت تصادفی ECP) نیاز خواهد بود. در صورتی‌که گروه DH اضافی مشخص گردید، این گروه‌ها باید مطابق الزامات لیست شده در رز-اپ.۱(۲) باشند.

۲۶ **نام عنصر: پروتکلIPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۸,۱ (FCS_IPSEC_EXT.1.8)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که تمام پروتکل‌های IKE با استفاده از کلیدها ی از پیش به اشتراک گذاشته شده و [انتخاب: DSA، rDSA، ECDSA] احراز هویت همتا را انجام می‌دهند و از گواهینامه‌ی X.509v3 مطابق با RFC 4945 جهت احراز هویت استفاده می کنند.

نکته کاربردی:

شماره	نام خانواده	عنصر امنیتی
الزام		

برای هدف ارزیابی منطبق بر این پروفایل حفاظتی به کلیدهای از پیش به اشتراک گذاشته شده و حداقل یک کلید عمومی مبتنی بر سازوکار احراز هویت همتا نیاز می‌باشد. توسط نویسنده هدف امنیتی یک یا بیش از یک طرح کلید عمومی انتخاب می‌شود تا آنچه را که توسط هدف ارزیابی پیاده‌سازی شده است منعکس کند. نویسنده هدف امنیتی هم‌چنین اطمینان می‌دهد که الزامات کلاس رمزنگاری (رز) الگوریتم‌های استفاده شده را (و در صورت ارائه ، قابلیت کلیدهای تولید شده) لیست می کند تا آن سازوکارها را پشتیبانی کند.

۲۷ **نام عنصر: پروتکلIPsec ۱**

شماره مؤلفه: رز-اپ-(ت‌س).۹,۱.(FCS_IPSEC_EXT.1.9)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید بتوانند به صورت پیش‌فرض اطمینان دهند که الگوریتم متقارن پیشنهاد شده جهت حفاظت اتصال [انتخاب: فاز ۱ IKEv1، IKEv2 IKE_SA] از نظر قدرت بزرگتر یا معادل الگوریتم متقارن (تعداد بیت‌های کلید) پیشنهاد شده جهت حفاظت اتصال [انتخاب: فاز ۲ IKEv1، IKEv2 CHILD_SA] می‌باشند.

نکته کاربردی:

نویسنده هدف امنیتی براساس آنچه که توسط هدف ارزیابی پیاده‌سازی شده است یک یا هر دوی پروتکل IKE را انتخاب می کند.

شماره	نام خانواده	عنصر امنیتی
الزام		
		بدیهی است که نسخه IKE انتخاب شده نه تنها باید در این مؤلفه سازگار باشد بلکه باید با دیگر عناصر این مؤلفه نیز سازگار باشد.
۲۸		**نکته کاربردی FCS_IPSEC_EXT.1:**
		این عنصر به صورت حداقلی برای محافظت از ارتباطات RADIUS بین سامانه دسترسی WLAN و سرور احراز هویت پشتیبانی شده است. اولین انتخاب برای شناسایی دیگر الگوریتم‌های رمزنگاری پشتیبانی شده، استفاده می‌شوند. از یکی از دو پروتکل IKEv1 و IKEv2 باید پشتیبانی شود هرچند هدف‌های ارزیابی مطابق با این پروفایل حفاظتی می‌توانند از هردوی این پروتکل‌ها پشتیبانی کنند. برای پروتکل IKEv1، الزام به صورتی که مورد نیاز پیاده‌سازی IKE منطبق بر RFC 2409 با تغییرات/اضافات توصیف شده در RFC 4109 می‌باشد، تفسیر می‌شود RFC 4868 توابع درهم‌سازی بیشتری برای استفاده هرد و پروتکل IKEv1 و IKEv2 تعریف نموده است. اگر این توابع پیاده‌سازی شده باشند، سومین انتخاب (برای IKEv1) و چهارمین انتخاب (برای IKEv2) می‌تواند استفاده شود. آخرین اختصاص/انتخاب برای مشخص نمودن دیگر سرورها/سرویس‌هایی (به طور مثال یک سرور ممیزی) استفاده می‌شود تا هدف ارزیابی با دیگر ارتباطاتی که توسط IPsec محافظت شده است، مرتبط شود.

۷,۳ کلاس حفاظت از داده‌های کاربری

در ادامه مؤلفه‌های امنیتی مورد نیاز حوزه حفاظت از داده‌های کاربری ارائه شده است.

نام کلاس: حفاظت از داده کاربری

شرح کلاس: این کلاس شامل خانواده‌هایی است که الزامات مربوط به محافظت از داده کاربر را مشخص می‌کنند: خانواده‌های محافظت از داده کاربر در چهار گروه زیر دسته بندی شده‌اند، که علاوه بر مشخصه‌های امنیتی مربوط به داده کاربری، داده‌های کاربری در داخل هدف ارزیابی را در طول ورود، خروج و ذخیره سازی نیز آدرس‌دهی می‌کنند.

خانواده‌های این کلاس در چهار گروه زیر دسته بندی شده‌اند:

۱) خط‌مشی‌های امنیتی مربوط به محافظت از داده کاربری

- خط‌مشی‌های کنترل دسترسی (حف-س‌ک)[1]
- خط‌مشی‌های مرتبط با کنترل جریان اطلاعات (حف-خج)[2]

در این دو خانواده، به نویسنده هدف امنیتی/پروفایل حفاظتی اجازه داده می‌شود تا خط‌مشی‌های امنیتی که برای حفاظت از داده‌کاربری در نظر گرفته شده، و همچنین حوزه کنترلی این خط‌مشی‌ها نام برده شود.

خط‌مشی‌های امنیتی نام برده شده در این دو خانواده

- خط‌مشی‌های امنیتی در نظر گرفته شده برای کنترل دسترسی
- خط‌مشی‌های امنیتی در نظر گرفته شده برای کنترل جریان اطلاعات

توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش «انتخاب» یا «اختصاص» فراخوانی می‌شوند.

در دو خانواده‌ی توابع کنترل دسترسی (حف-ت‌ک)[1] و توابع کنترل جریان اطلاعات (حف-کج)[2] قوانینی که تعریف کننده‌ی « خط‌مشی‌های امنیتی کنترل دسترسی» و « خط‌مشی‌های امنیتی کنترل جریان اطلاعات» هستند، آورده شده است.

---

1 Access control policy(FDP_ACC)

2 Information flow control policy(FDP_IFC)

۲) فرم‌های مختلف محافظت از داده کاربری

- توابع کنترل دسترسی (حف-ت‌ک)
- توابع کنترل جریان اطلاعات (حف-ک‌ج)
- انتقال داخلی در هدف ارزیابی (حف-اد)[۳]
- حفاظت از اطلاعات باقیمانده (حف-اب)[۴]
- عملیات عقب‌گرد به منظور بازگرداندن حالت/حالت‌های قبل (حف-ع‌گ)[۵]
- یکپارچگی داده‌های ذخیره شده (حف-ی‌د)[۶]

۳) ورود و خروج، ذخیره‌سازی برون‌خطی[۷]

- احراز هویت[۱] داده (حف-ت‌د)

---

1 Access control functions(FDP_ACF)

2 Information flow control functions(FDP_IFF)

3 Internal TOE transfer(FDP_ITT)

4 Residual information protection(FDP_RIP)

5 Rollback(FDP_ROL)

6 Stored data integrity(FDP_SDI)

7 Offline

- صادر شده از هدف ارزیابی (حف-ص‌ا)[۲]
- ورود داده‌ها از بیرون به هدف ارزیابی (حف-وب)[۳]

مؤلفه‌های این خانواده، انتقال قابل اعتماد به داخل یا خارج از هدف ارزیابی را آدرس‌دهی می‌کنند.

۴) ارتباطات میان توابع امنیتی هدف ارزیابی

- محافظت از انتقال محرمانگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-مد)[۴]
- محافظت از انتقال یکپارچگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(حف-ی‌ا)[۵]

مؤلفه‌های این خانواده ارتباطات بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن فناوری اطلاعات را آدرس‌دهی می‌کند.

➢ خانواده خط‌مشی‌های کنترل دسترسی

این خانواده خط‌مشی‌های امنیتی مربوط به کنترل دسترسی را نام می‌برد و حوزه کنترلی سیاست‌گذاری‌ها را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال[۱] تحت کنترل سیاست‌گذاری‌ها

---

1 Data authentication(FDP_DAU)

2 Export from the TOE(FDP_ETC)

3 Import from outside of the TOE(FDP_ITC)

4 Inter-TSF user data confidentiality transfer protection(FDP_UCT)

5 Inter-TSF user data integrity transfer protection(FDP_UIT)

- موجودیت‌های غیرفعال[2] تحت کنترل سیاست‌گذاری‌ها
- عملیات بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده که توسط خط‌مشی‌های امنیتی پوشش داده می‌شود.

بنابراین در مؤلفه‌های این خانواده، خط‌مشی امنیتی نامبرده می‌شود و برای هریک از خط‌مشی‌های امنیتی نامبرده شده، موجودیت فعال و غیرفعال تحت کنترل آن خط-مشی و عملیات بین موجودیت فعال و غیرفعال نیز نامبرده می‌شود.
در این خانواده می‌توان خط‌مشی‌های امنیتی مختلفی برای کنترل دسترسی داشت، و هریک نام منحصر به فرد خود را داشته باشند تنها باید مؤلفه‌های این خانواده برای هر یک از خط‌مشی‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-س‌ک.۱٫۱(۱)، حف-س‌ک.۱٫۱(۲)).
قوانینی که عملکرد خط‌مشی‌های امنیتی را برای کنترل دسترسی تعریف می کنند، در خانواده‌های توابع کنترل دسترسی (حف-ت‌ک) و صادر شده از هدف ارزیابی (حف-ص‌ا) تعریف می‌شوند.
خط‌مشی‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش «انتخاب» یا «اختصاص» فراخوانی می‌شوند.

➢ خانواده توابع کنترل دسترسی

در خانواده خط‌مشی‌های امنیتی کنترلی دسترسی (حف-س‌ک)، تنها این خط‌مشی‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای خط‌مشی امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (حف-س‌ک)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل خط‌مشی‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام برده می‌شوند.

➢ خانواده احراز هویت داده

---

1 Subject
2 Object

احراز هویت داده به هر نهادی، اجازه‌ی پذیرش مسوولیت احراز صحت اطلاعات را می‌دهد (با دیجیتالی امضاء نمودن اطلاعات). این خانواده روشی را مشروط بر تضمین اعتبار یک بخش خاص از داده ارائه می‌کند که می‌تواند به منظور بررسی محتوای اطلاعات از لحاظ جعل نشدن یا تغییر یافتن مکرر مورد استفاده قرار گیرد.

- **خانواده صادرشده از هدف ارزیابی**

در دو خانواده (حف-س‌ک) و (حف-خج) خط‌مشی‌های امنیتی بر روی کنترل دسترسی و جریان اطلاعات نام برده شده‌اند. در این خانواده این خط‌مشی‌های امنیتی بر روی داده تحت کنترل این خط‌مشی‌ها هنگام خروج از هدف ارزیابی اعمال می‌شود، مشخصه‌های امنیتی داده‌ها هنگام صدور می‌تواند حفظ شوند یا نادیده گرفته شوند. در واقع در این خانواده محدودیت‌هایی برای صدور داده از هدف ارزیابی اعمال می‌شود.

- **خط‌مشی‌های کنترل جریان اطلاعات**

این خانواده سیاست‌گذاری‌های عملکرد امنیتی مربوط به کنترل جریان اطلاعات را نام می‌برد و برای هریک از آنها، حوزه کنترلی را تعریف می‌کند. این حوزه کنترلی توسط سه مجموعه زیر مشخص می‌شود:

- موجودیت‌های فعال تحت کنترل سیاست‌گذاری‌ها
- اطلاعات تحت کنترل سیاست‌گذاری‌ها
- عملیاتی که سبب کنترل اطلاعات جریان یافته به/از موجودیت‌های فعال کنترل شده تحت پوشش این خط‌مشی‌ها می‌باشند.

بنابراین در مؤلفه‌های این خانواده، خط‌مشی امنیتی نام‌برده می‌شوند و برای هریک از خط‌مشی‌های امنیتی نامبرده شده، موجودیت فعال و غیرفعال تحت کنترل آن خط-مشی و عملیات بین موجودیت فعال و غیرفعال نیز نام برده می‌شوند.
در این خانواده می‌توان خط‌مشی‌های امنیتی مختلفی برای کنترل دسترسی داشت، و هریک نام منحصر به فرد خود را داسته باشند تنها باید مؤلفه‌های این خانواده برای هریک از خط‌مشی‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-خج.۱,۱(۱)، حف-خج.۱,۱(۲)).

قوانینی که عملکرد خط‌مشی‌های امنیتی را برای کنترل دسترسی تعریف می‌کنند، در خانواده‌های توابع کنترل دسترسی (ح‌ف-ک‌ج) و صادر شده از هدف ارزیابی (ح‌ف-ص‌ا) تعریف می‌شوند.
خط‌مشی‌های نام برده شده در این خانواده توسط مؤلفه‌های دیگر خانواده‌ها با استفاده از بخش «انتخاب» یا «اختصاص» فراخوانی می‌شوند.

- **خانواده توابع کنترل جریان اطلاعات**

در خانواده خط‌مشی‌های امنیتی کنترلی دسترسی (ح‌ف-خ‌ج)، تنها این خط‌مشی‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای خط‌مشی امنیتی بر روی عملیات بین موجودیت‌های فعال و غیرفعال (نام برده شده در خانواده (ح‌ف-خ‌ج)) وضع می‌شود. هم‌چنین در این خانواده موجودیت‌های فعال و غیرفعال تحت کنترل خط-مشی‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام برده می‌شوند.این خانواده شامل دو الزام است:

- یکی پرداختن به مسائل عملکرد جریان اطلاعات رایج
- پرداختن به جریان اطلاعات غیرمجاز

این تقسیم‌بندی به این دلیل مطرح شده است که مسائل مربوط به جریان اطلاعات غیرمجاز، در برخی موارد با باقی سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات در تعامد است. با توجه به طبیعتشان سرپیچی نمودن آنها از سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات، منجر به نقص در خط‌مشی‌ها می‌شود. بنابراین، باید عملیات‌های خاصی برای جلوگیری یا محدود نمودن جریان اطلاعات غیرمجاز در نظر گرفت.

- **خانواده ورود داده‌ها از بیرون به هدف ارزیابی**

این خانواده تعریف کننده سازوکارهایی برای ورود داده‌های کاربری تحت کنترل خط‌مشی‌های امنیتی (خط‌مشی‌های امنیتی کنترل جریان و کنترل دسترسی) از خارج هدف ارزیابی می‌باشد. برای ورود داده باید خط‌مشی‌های تعریف شده بر روی داده اعمال شود، هم‌چنین مشخصه های امنیتی مطلوبی برای اینگونه از داده‌ها در نظر گرفته می‌شود. در واقع این خانواده محدودیت‌هایی بر روی داده‌های ورودی از خارج هدف ارزیابی اعمال می‌کند.

- **خانواده انتقال هدف ارزیابی داخلی**

این خانواده الزاماتی را ارائه می‌دهد تا از داده کاربری در زمانی‌که بین بخش‌های مجزای هدف ارزیابی در سراسر کانال داخلی[1] انتقال می‌یابد، حفاظت کند. هم‌چنین در این خانواده داده‌ها براساس مشخصه‌های امنیتی از یکدیگر مجزا می‌شوند و برای شناسایی خطا در صحت داده، داده‌های منتقل شده بین بخش‌های هدف ارزیابی پایش می‌شوند.

- **خانواده حفاظت از اطلاعات باقیمانده**

این خانواده اطمینان می‌دهد در زمانی‌که منبع از یک موجودیت غیرفعال آزاد می‌شود و دوباره به یک موجودیت غیرفعال دیگر اختصاص داده می‌شود، هرگونه داده موجود در منابع، در دسترس قرار نمی‌گیرد. این خانواده نیاز دارد که از هرگونه داده موجود در منابع که به طور منطقی حذف یا آزاد می‌شود، محافظت کند، اما ممکن است هنوز در داخل منابع کنترل شده توابع امنیتی هدف ارزیابی اطلاعاتی وجود داشته باشد که به موجودیت غیرفعال دیگری اختصاص داده شود.

- **خانواده عملیات عقب‌گرد به منظور بازگرداندن حالت/ حالت‌های قبل**

عملکرد عقب‌گرد شامل بی‌اثر نمودن آخرین عملکرد یا یک سری از عملکردها، محدود شدن به برخی محدودیت‌ها هم‌چون بازه زمانی و برگشت به یک وضعیت شناخته شده قبلی می‌باشد. عقب‌گرد فراهم کننده‌ی قابلیت بی‌اثر نمودن عملیات یا مجموعه‌ای از عملیات است تا یکپارچگی داده کاربری را حفظ کند.

- **خانواده صحت داده‌های ذخیره شده**

این خانواده الزاماتی را ارائه می‌کند که از داده کاربری ذخیره شده در کانتینر تحت کنترل توابع امنیتی هدف ارزیابی، محافظت می‌کند. خطای صحت ممکن است داده کاربری ذخیره شده در حافظه یا در یک ابزار ذخیره‌سازی را تحت تاثیر قرار بدهند. این خانواده صحت داده‌های ذخیره شده را حفظ می‌کند و ممکن است در صورت تشخیص خطا، اقدامی در برابر آن انجام بدهد،اما خانواده «انتقال هدف ارزیابی داخلی (حف-اد)» صحت داده کاربری در حال انتقال در هدف ارزیابی را محافظت می‌کند.

---

1 Internal channel

- **خانواده محافظت از انتقال محرمانگی داده کاربر در توابع امنیتی هدف ارزیابی داخلی**

این خانواده تعریف کننده الزاماتی است که محرمانگی داده کاربری را در زمانی‌که با استفاده از یک کانال خارجی بین هدف ارزیابی و دیگر محصولات امن IT انتقال می‌یابد، تضمین می‌کند.

- **خانواده محافظت از انتقال صحیح داده کاربر در داخلی عملکرد امنیتی هدف ارزیابی**

این خانواده الزاماتی را تعریف می‌کند تا صحت داده کاربری را که بین هدف ارزیابی و دیگر محصولات امن IT منتقل می‌شود، تأمین کند و داده کاربری را از خطاهای قابل تشخیص بازیابی کند. این خانواده حداقل داده کاربری را جهت اطمینان از تغییر نیافتن پایش می‌کند. همچنین، این خانواده از روش‌های مختلف جهت اصلاح خطاهای تشخیص داده شده در صحت داده پشتیبانی می‌کند.

شماره الزام	نام خانواده	عنصر امنیتی
۲۹	حفاظت از داده های باقی مانده **(FDP_RIP)**	**نام عنصر:** حفاظت کامل از داده های باقی مانده ۲ **شماره مؤلفه:** ح‌ف‌-اب.۱,۲(FDP_RIP.2.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تضمین کنند که هرگونه محتوی اطلاعات قبلی یک منبع را در زمان [انتخاب: تخصیص منابع به،

شماره	نام خانواده	عنصر امنیتی
الزام		

آزادسازی منابع از] تمام موجودیت های غیرفعال، غیرقابل دسترس کنند.

۷,۴ کلاس شناسایی و احراز هویت

نام کلاس: ممیزی امنیت

شرح کلاس: سامانه های تشخیص نفوذ برای رخدادهای گوناگون اقدام به ایجاد گزارشهایی برای ممیزی می‌کنند. کلاس ممیزی امنیت، الزاماتی پیرامون نحوه شناخت، ثبت و ذخیره و آنالیز اطلاعات ممیزی مربوط به فعالیت‌های مرتبط امنیتی تعریف نموده است (فعالیت‌هایی که توسط توابع امنیتی هدف ارزیابی کنترل می‌شوند). با بررسی ممیزی‌های ثبت شده می‌توان تعیین کرد کدام رخداد مرتبط با چه فعالیت امنیتی صورت گرفته و چه‌کسی (چه کاربری) مسوول آن است. این کلاس شامل ۵ خانواده است که عبارتند از:

- **خانواده پاسخ سامانه در برخورد با خطاهای امنیتی[1]**

این خانواده تعریف کننده الزامات برای واکنش‌های سامانه نسبت به رویدادهایی است که بروز آنها نشان‌دهنده نقض امنیتی بالقوه‌ای باشد.

- **خانواده تولید داده ممیزی[2]**

1 Security audit automatic response (FAU_ARP)

2 Security audit data generation (FAU_GEN)

این خانواده الزاماتی برای ثبت رخدادهای امنیتی مربوط به رویدادهایی را که تحت کنترل توابع امنیتی هدف ارزیابی صورت می‌گیرند تعریف می‌کند. این خانواده سطح ممیزی را تعیین می‌کند، انواع رویدادهایی که بایستی توسط توابع امنیتی هدف ارزیابی قابل ممیزی باشند را بیان می‌کند و یک مجموعه حداقلی از اطلاعات مرتبط با ممیزی را تعیین می‌کند که باید در داخل انواع ممیزی‌های امنیتی ثبت شده، ارائه شوند.

- **خانواده تحلیل ممیزی امنیت[1]**

این خانواده الزاماتی برای ابزارهای خودکار، که فعالیت‌های سامانه را تحلیل می‌کند و داده‌های ممیزی که نقص امنیتی واقعی یا ممکن را جستجو می‌کنند، تعریف می‌کند. این تحلیل ممکن است در پشتیبانی از تشخیص نفوذ، یا پاسخ خودکار به نقص امنیتی بالقوه کار کند.

- **خانواده بازبینی ممیزی امنیت[2]**

این خانواده تعریف کننده الزاماتی برای ابزارهای ممیزی است که باید در دسترس کاربران مجاز قرار بگیرند تا به بازبینی داده‌های ممیزی کمک کند.

- **خانواده انتخاب رویدادهای ممیزی امنیت[3]**

این خانواده تعریف کننده الزاماتی جهت انتخاب یک مجموعه رویدادهای ممیزی شده در طول عملکرد هدف ارزیابی، از بین تمام رویدادهای قابل ممیزی می‌باشد.

- **خانواده ذخیره‌سازی رویدادهای ممیزی امنیت[4]**

1 Security audit analysis (FAU_SAA)
2 Security audit review (FAU_SAR)
3 Security audit event selection (FAU_SEL)
4 Security audit event storage (FAU_STG)

این خانواده تعریف کننده الزاماتی برای توابع امنیتی هدف ارزیابی است تا قادر به ایجاد و نگهداری از سوابق ممیزی بصورت امن باشند.

شماره الزام	نام خانواده	عنصر امنیتی
۳۰	شکست‌ها در احراز هویت (FIA_AFL)	**نام عنصر: مدیریت احراز هویت ناموفق[1] ۱** **شماره مؤلفه: اش-ش.۱.۱** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی، باید [اختصاص: **یک عدد مثبت قابل تنظیم و غیر صفر**]از تلاش‌های ناموفق احراز هویت را نسبت به آخرین احراز هویت موفق مشخص کنند. **نکته کاربردی:** • هدف ارزیابی ممکن است برای کاربران مختلف، متدهای احراز هویت متفاوتی استفاده کند و از قوانین مختلفی براساس متدهای احراز هویت/ یا کاربران جهت مدیریت نمودن احراز هویت ناموفق بهره بگیرد. رفتاری که در قبال احراز هویت ناموفق، برای سامانه‌های از راه دور و کاربران انسانی صورت می‌گیرد، معمولاً متفاوت از هم می‌باشد. حتی برای کاربران انسانی

1 Authentication failures (FIA_AFL)

شماره الزام	نام خانواده

عنصر امنیتی

ممکن است، عکس‌العمل در برابر احراز هویت ناموفق برای احراز هویتی که از طریق نام کاربری/رمزعبور صورت می‌گیرد نسبت به احراز هویتی که از طریق کارت هوشمند یا گواهینامه‌های دیجیتال انجام می‌گیرد، متفاوت باشد.

- رویداد احراز هویت ناموفق با توجه به آخرین نشست موفق در ترمینال شمارش می‌شود.

هرچند که لیستی از اقدامات می‌تواند توسط هدف ارزیابی، مشخص شود. اما این مجموعه اقدامات باید اطمینان دهد که از حملات مبتنی بر جستجو در فضاهای ممکن جلوگیری می‌کند.

۳۱ **نام عنصر: مدیریت احراز هویت ناموفق ۱**

شماره مؤلفه: اش-ش‌ا.۲,۱

شرح مؤلفه:

زمانی‌که تعداد تلاش‌های ناموفق صورت گرفته برای احراز هویت به حد معینی رسید یا از آن بیشتر شد، توابع امنیتی هدف ارزیابی باید [انتخاب:

جلوگیری سرپرست متخلف در احراز هویت با موفقیت، تا زمانی‌که [اختصاص: اقدام] توسط سرپرست مجاز

شماره الزام	نام خانواده عنصر امنیتی	

صورت بگیرد.؛

جلوگیری نمودن از سرپرست متخلف در احراز هویت نمودن با موفقیت، تا زمانی‌که سرپرست مجاز مدت زمان مجاز تعریف شده را سپری کند.]

انجام دهد.

نکته کاربردی:

این الزامات به سرپرست در کنسول محلی اعمال نمی‌شود، از این‌رو ممکن است سبب قفل نمودن حساب سرپرست محلی در این مدل شود. این امر می‌تواند (برای مثال) با درنظر گرفتن یک حساب جداگانه برای سرپرست محلی یا با داشتن سازوکار احراز هویتی که تلاش‌های برای ورود از راه دور و محلی را مجزا از هم پیاده‌سازی می‌کند. «اقدام» صورت گرفته توسط سرپرست یک پیاده‌سازی خاص است و در راهنمای سرپرستی تعریف می‌شود (برای مثال، تنظیم مجدد قفل یا تنظیم مجدد رمزعبور). نویسنده هدف امنیت یکی از انتخاب‌ها را جهت کنترل شکست‌های احراز هویت انتخاب می کند با توجه به آنکه چگونه هدف ارزیابی این کنترل کننده را پیاده‌سازی نموده است.

شماره	نام خانواده	عنصر امنیتی
الزام		
۳۲	مدیریت رمز عبور (FIA_PMG_EXT)	**نام عنصر: مدیریت رمز عبور ۱** **شماره مؤلفه: اش-مع.(تس).۱,۱ (FIA_PMG_EXT .1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیت‌های مدیریت رمزعبور را که در زیر ذکر شده‌اند برای رمزهای عبور سرپرستی فراهم کند:

۱. رمزهای عبور باید بتوانند هرترکیبی ازحروف کوچک و بزرگ، اعداد و کاراکترهای خاص: [انتخاب: "@"، "#"، "$"، "٪"، "^"، "!" "&"، "*"، "(" , ")" [,اختصاص: کاراکتر دیگر]] باشند.

۲. حداقل طول رمزعبور باید توسط سرپرست امنیت، قابل تنظیم بوده و ۸ کاراکتر یا بیشتر باشد.

۳. قوانین ترکیب رمزعبور نوع و تعداد کاراکترهای مورد نیاز را مشخص می‌کند که شامل رمزعبورهایی است که باید توسط سرپرست تنظیم شود.

۴. رمزهای عبور باید دارای حداکثر طول عمر باشد که توسط سرپرست مجاز تنظیم می‌شود.

۵. رمزعبور جدید باید حداقل در چهار کاراکتر متفاوت از رمزعبور قبلی باشد.

شماره الزام	نام خانواده	عنصر امنیتی

نکته کاربردی:

لازم به ذکر است که نیازی به ذخیره یک نسخه متنی از رمزعبور به منظور تعیین حداقل ۴ کاراکتر تغییر کرده نمی‌باشد، زیرا با توجه به الزام اش-اه.۶ در زمان تغییر رمزعبور نیاز به احراز هویت مجدد می‌باشد.

"رمزعبور سرپرستی" به رمزعبورهایی اشاره دارد که توسط سرپرست در کنسول محلی یا بر روی پروتکل‌هایی هم‌چون SSH و HTTPS که رمزعبور را پشتیبانی می کنند، استفاده می‌شوند.

منظور از مورد سوم در الزام بالا آن است که سرپرست مجاز قادر به مشخص نمودن است، برای مثال، رمز عبور شامل حداقل یک کاراکتر بزرگ، یک کاراکتر کوچک، یک کاراکتر عددی و یک کاراکتر خاص است و هدف ارزیابی این محدودیت‌ها را اجرا می‌کند. «نوع» اشاره به تمام انواع لیست شده در اولین مورد در این مؤلفه دارد.

۳۳	شناسایی و احراز هویت کاربر	**نام عنصر: شناسایی و احراز هویت کاربر ۱** **شماره مؤلفه: اش-ش‌ه.۱،۱ (FIA_UIA_EXT .1.1)**

شماره	نام خانواده	عنصر امنیتی
الزام		
(FIA_UIA_EXT)		**شرح مؤلفه:**

توابع امنیتی هدف ارزیابی، باید پیش از آنکه نیاز به موجودیت‌های غیرهدف ارزیابی، جهت شروع رویه شناسایی و احراز هویت باشد، اقدامات زیر را مجاز کند:

- نمایش هشدارها مطابق با خانواده "دس_ع د.۱"
- [اختصاص: لیستی از سرویس‌ها، اقداماتی که توسط توابع امنیتی هدف ارزیابی جهت پاسخ دادن به در خواست‌های «غیر هدف ارزیابی» صورت می‌گیرد.]

۳۴

نام عنصر: شناسایی و احراز هویت کاربر ۱

شماره مؤلفه: اش-ش‌ه.۲,۱ (FIA_UIA_EXT .1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی، باید پیش از آنکه به هر اقدام میانی از سوی سرپرست اجازه داده شود، هر سرپرست را ملزم به شناسایی و احرازهویت موفق کند.

نکته کاربردی:

شماره الزام	نام خانواده	عنصر امنیتی

این الزامات به کاربران سرویس‌هایی اعمال می‌شود که از هدف ارزیابی مستقیماً قابل دسترس است و شامل سرویس‌هایی که با اتصال از طریق هدف ارزیابی در دسترس قرار می‌گیرند، نمی‌شود. در حالی‌که باید هیچ سرویس و یا سرویس‌های کمی پیش از شناسایی و احراز هویت در دسترس موجودیت‌های خارجی باشند، در صورت وجود چنین سرویس‌هایی باید در قسمت «اختصاص» لیست شوند، در غیر این‌صورت «بدون هیچ اقدام دیگر» انتخاب می‌شود.

احراز هویت می‌تواند براساس رمزعبور از طریق یک کنسول محلی یا پروتکلی باشدکه از چنین رمزهای عبوری پشتیبانی می‌کند (هم‌چون SSH)، یا براساس گواهینامه (SSH,TLS) باشد.

برای ارتباط با یک موجودیت IT خارجی (برای مثال سرور ممیزی، یا NTP سرور) چنین اتصالاتی باید مطابق با م م_ک م.۱ صورت گیرد، چنبن پروتکل هایی شناسایی و احراز هویت انجام می‌دهند.

۳۵	احرازهویت کاربر **(FIA_UAU)**	**نام عنصر:**سازوکار احراز هویت مبتنی بر رمزعبور **۵**

شماره مؤلفه: اش-اه.**۱,۵ (FIA_UAU_EXT.5.1)**

شرح مؤلفه:

شماره	نام خانواده
الزام	

عنصر امنیتی

توابع امنیتی هدف ارزیابی باید جهت احراز هویت کاربران، سازوکار احرازهویتی مبتنی بر رمز عبور،([انتخاب: [اختصاص: دیگر سازوکارهای احرازهویت]، هیچ‌کدام] ارائه دهد.

نکته کاربردی:

این الزام تنها به ثبت ورود سرپرست محلی اعمال می‌شود، و اساساً مستلزم آن است که یک سازوکار مبتنی بر رمز عبور برای این منظور بر روی هدف ارزیابی وجود داشته باشد. نویسنده هدف امنیتی می‌تواند قسمت «اختصاص» را با هر سازوکار دیگری که از احرازهویت پشتیبانی می‌شود (همانند سرور احراز هویت) برای سرپرستانی که محلی نیستند، تکمیل کند. اگر هیچ سازوکار دیگری برای سرپرست محلی پشتیبانی نشود، نویسنده هدف امنیتی باید در قسمت «انتخاب» هیچکدام را برگزیند.

۳۶

نام عنصر:سازوکار احراز هویت مبتنی بر رمزعبور **۵**

شماره مؤلفه: اش-اه.**۱,۵ (FIA_UAU_EXT.5.1)**

شرح مؤلفه:

شماره **نام خانواده**

الزام

عنصر امنیتی

توابع امنیتی هدف ارزیابی باید اطمینان دهد که سرپرستانی با رمزعبور منقضی شده [انتخاب: نیاز به ایجاد رمزعبور جدید پس از وارد نمودن رمز عبور منقضی شده به طور صحیح دارند، تا زمانی‌که رمزعبورشان توسط سرپرست دوباره تنظیم شود، قفل می‌شوند.]

۳۷

نام عنصر:احراز هویت مجدد **۶**

شماره مؤلفه: اش-اه.**۱,۶ (FIA_UAU_EXT.5.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید تحت شرایط زیر، سرپرست را مجدداً احراز هویت کند:

زمانی‌که کاربر رمز عبورش را تغییر می‌دهد، [انتخاب: پس از قفل شدن آنهایی که توسط توابع امنیتی هدف ارزیابی آغاز شده‌اند(دس-ق‌ن)، [اختصاص: دیگر شرایط] ، هیچ شرایط دیگر].

۳۸

نام عنصر:احراز هویت مجدد **۷**

شماره	نام خانواده	عنصر امنیتی
الزام		

شماره مؤلفه: اش-اه.**۱,۷ (FIA_UAU_EXT.7.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید زمانی‌که فرآیند احراز هویت، در کنسول محلی در حال صورت گرفتن است؛ تنها به سرپرست بازخورد مبهمی[1] ارائه دهند.

نکته کاربردی:

«بازخورد مبهم» نشان می‌دهد که توابع امنیتی هدف ارزیابی، نمایش واضحی از هر داده‌ای که جهت احراز هویت شدن توسط کاربر وارد می‌شود، ندارند(مانند انعکاس رمز عبور). هر چند «بازخورد مبهم» از روند احراز هویت ممکن است ارائه شود(همچون * که در زمان وارد نمودن هر کاراکتر توسط کاربر، نشان داده می‌شود). «بازخورد مبهم» همچنین نشان می‌دهد که توابع امنیتی هدف ارزیابی، هیچ اطلاعاتی را در طول رویه احراز هویت به کاربر برنمی‌گردانند.

۳۹	پروتکل	802.1X	**نام عنصر: احرازهویت موجودیت دستیابی به پورت 802.1X ۱**

1 Obscured feedback

شماره الزام	نام خانواده عنصر امنیتی
(FIA_8021X_EXT)	شماره مؤلفه: اش-۱,۱.8021X (FIA_8021X_EXT .1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید مطابق با استاندارد IEEE 802.1X برای موجودیت دستیابی به پورت (PAE) در نقش «درخواست کننده» باشد.

نکته کاربردی:

این الزام نقش هدف ارزیابی را به عنوان درخواست کننده در تبادلات احراز هویت 802.1X پوشش می‌دهد. اگر تبادلات موفقیت آمیز به پایان برسد، هدف ارزیابی در اثر پروتکل EAP-TLS کلید PMK را استنتاج می-کند (یا دیگر تبادلات EAP مناسب) و یک دست‌دهی [1]چهار طرفه با سامانه دستیابی بدون سیم انجام می-دهد (احراز کننده) تا ارتباط 802.11 شروع شود.

همان‌طور که قبلاً نشان داد شده است، حداقل دو مسیر ارتباطی در طول تبادل وجود دارد، یکی با سامانه دستیابی بی‌سیم و دیگری با سرور احراز هویت که از سامانه دستیابی بی‌سیم به صورت رله استفاده می‌کند.

1 Handshake

شماره الزام **نام خانواده**

عنصر امنیتی

هدف ارزیابی یک EAP بر روی اتصال LAN با سامانه دستیابی بی‌سیم به صورت مشخص شده در 802.1X-2010 ایجاد می‌کند. هدف ارزیابی یک اتصال پروتکل RADIUS(که درداخل اتصال IPsec تونل شده است) را با سرور RADIUS برقرار می‌کند. کلاینت وایرلس و سرور RADIUS یک نشست EAP-TLS برقرار می‌کنند (RFC 5216). در این تراکنش هدف ارزیابی صرفاً بسته EAP-TLS از نقطه پایانی EAPOL/RADIUS را می‌گیرد و به نقطه پایانی دیگر منتقل می‌کند. از آنجا که سازوکار احراز هویت خاص (TLS در این مورد) برای هدف ارزیابی مبهم است، هیچ الزامی با توجه به RFC 5126 در این پروفایل حفاظتی وجود ندارد. با این حال، پروتکل RADIUS پایه (2865) به روزرسانی (3579) دارد که نیاز خواهد داشت که در پیاده‌سازی و فعالیت-های تضمین آدرس‌دهی شود. علاوه بر این، RFC 5080 شامل انواع پیاده‌سازی است که نیاز خواهد بود توسط توسعه دهندگان آدرس‌دهی شود، اما هیچ الزام جدیدی را تحمیل نمی‌کند. نقطه انجام احراز هویت 802.1X دستیابی به شبکه را فراهم می‌آورد.(با فرض احراز هویت موفق و اینکه تمام مذاکرات 802.11 موفقیت‌آمیز انجام شود)؛ در اصطلاحات پروتکل 802.1X، بدان معناست که کلاینت بی‌سیم به «پورت کنترل شده‌ای» دسترسی دارد که توسط هدف ارزیابی نگهداری می‌شود.

شماره	نام خانواده	عنصر امنیتی
الزام		
۴۰		**نام عنصر: احرازهویت موجودیت دستیابی به پورت 802.1X ۱** **شماره مؤلفه: اش-802.1X,۱,۲ (FIA_8021X_EXT .1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از ارتباط با سرور احراز هویت RADIUS مطابق با RFC 2865 و RFC 3579 پشتیبانی کنند.
۴۱		**نام عنصر: احرازهویت موجودیت دستیابی به پورت 802.1X ۱** **شماره مؤلفه: اش-802.1X,۱,۳ (FIA_8021X_EXT .1.3)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اطمینان بدهند که هیچ دسترسی از پورت کنترل شده‌ی 802.1X به کلاینت وایرلس پیش از اتمام موفقیت آمیز تبادلات احراز هویت داده نمی‌شود.
۴۲	کلید از پیش به اشتراک گذاشته شده (توسعه یافته)	**نام عنصر:** ترکیب کلیدهای از پیش به اشتراک گذاشته شده ۱ **شماره مؤلفه: اش-ت‌ک.۱,۱ (FIA_PSK_EXT.1.1)**

شماره الزام	نام خانواده	عنصر امنیتی
	(FIA_PSK_EXT)	

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر به استفاده از کلیدهای از پیش به اشتراک گذارده شده برای پروتکل IPsec و [انتخاب: هیچ پروتکل دیگر، [اختصاص: دیگر پروتکل‌هایی که از کلیدهای از پیش به اشتراک گذاشته شده استفاده می کنند]] باشد.

نکته کاربردی:

در اولین انتخاب، اگر پروتکل‌های دیگر بتوانند از کلیدهای از پیش به اشتراک گذاشته شده استفاده کنند، آنها باید در قسمت «اختصاص» لیست شوند، در غیر این‌صورت «هیچ پروتکل دیگر» باید انتخاب شود. منظور این الزام آن است که تمام پروتکل‌ها از هر دوی کلیدهای مبتنی بر متن و از پیش به اشتراک گذاشته شده پشتیبانی خواهند نمود.

اندازه کلید از پیش به اشتراک گذاشته شده مبتنی بر متن، جهت ترویج قابلیت همکاری به طول معمول (۲۲ کاراکتر) نیاز است. اگر اندازه‌های دیگری نیز پشتیبانی می‌شود باید در قسمت «اختصاص» لیست شوند. در قسمت "اختصاص" می‌توان یک محدوده از مقادیر (به طور مثال " اندازه از ۵ تا ۵۵ کاراکتر") را نیز

شماره الزام	نام خانواده عنصر امنیتی	
		مشخص نمود.
۴۳		**نام عنصر: ترکیب کلیدهای از پیش به اشتراک گذاشته شده ۱** **شماره مؤلفه: اش-ت‌ک.۲,۱ (FIA_PSK_EXT.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قادر به پذیرش کلیدهای از پیش به اشتراک گذاشته شده مبتنی بر متن باشد که: • ۲۲ کاراکتر می‌باشد و [انتخاب: [اختصاص: دیگر اندازه‌هایی که پشتیبانی می‌شود]، هیچ اندازه دیگر]. • ترکیبی از حروف بزرگ و کوچک، اعداد و کاراکترهای خاص (که شامل: "!"، "@"، "#"، "$"، "%"، "^"،"&"،"*"،")"،"("،"")
۴۴		**نام عنصر:** ترکیب کلیدهای از پیش به اشتراک گذاشته شده ۱ **شماره مؤلفه: اش-ت‌ک.۳,۱ (FIA_PSK_EXT.1.3)**

شماره الزام	نام خانواده

عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید کلیدهای از پیش به اشتراک گذاشته شده مبتنی بر متن را به استفاده از [انتخاب: SHA-1، SHA-256، SHA-512T، [اختصاص: سازوکار مقیدنمودن رشته متنی]] مقید کند.

۴۵ **نام عنصر:** ترکیب کلیدهای از پیش به اشتراک گذاشته شده ۱

شماره مؤلفه: اش-ت‌ک.۴,۱ (FIA_PSK_EXT.1.4)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر باشد کلیدهای از پیش به اشتراک گذاشته شده مبتنی بر بیت را [انتخاب: بپذیرد، با استفاده از تولید کننده بیت تصادفی (RBG)، مشخص شده در عنصر رز-ب‌ت.(ت‌س).۱ تولید کند].

نکته کاربردی:

نویسنده هدف امنیتی مشخص می کند که اساساً توابع امنیتی هدف ارزیابی کلیدهای از پیش به اشتراک گذاشته شده مبتنی بر بیت را می‌پذیرد یا قادر به تولید آنها می‌باشد. اگر آنها را تولید کند، این الزام مشخص

شماره الزام	نام خانواده	عنصر امنیتی
		می کند که این کلیدها باید توسط RBG که توسط هدف ارزیابی ارائه شده است، تولید شوند.
۴۶	خانواده گواهینامه-های X509 (FIA-X509)	**نام عنصر: گواهینامه‌های X509. ۱** **شماره مؤلفه: اش-X509 (ت‌س).۱,۱(FIA-X509-EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از گواهینامه‌های x509v3 به صورت تعریف شده در RFC 5280 استفاده کنند تا از احراز هویت برای IPsec و اتصالات [انتخاب: بدون پروتکل دیگر، TLS، SSH] پشتیبانی کنند. **نکته کاربردی:** نویسنده هدف امنیتی باید پروتکل‌هایی را انتخاب کند که در پیاده‌سازی اتصال‌های سرپرستی که از گواهینامه‌ها برای احرازهویت استفاده می‌کنند به کار می‌رود. باید توجه نمود که RFC 5280 الزامات اعتبارسنجی مسیر گواهینامه و اعتبارسنجی گواهینامه را تعریف می-کند که باید توسط هدف ارزیابی طبق این الزام پیاده‌سازی شود. باتوجه به پروتکل انتخاب شده، ممکن است الزامات (و فعالیت‌های مرتبط با تضیمن) مربوط به گواهینامه

شماره الزام	نام خانواده عنصر امنیتی
	پروتکل خاص مشخص شود (برای نمونه RFC 4945 برای پروتکل IPsec). این الزامات اضافی در الزامات مربوط به آن پروتکل مشخص شده است.
۴۷	**نام عنصر: گواهینامه‌های X509. ۱** **شماره مؤلفه: اش-X509 (ت‌س).۲,۱.(FIA-X509-EXT.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید گواهینامه‌ها را برای جلوگیری از حذف و تغییر غیرمجاز، ذخیره و محافظت کنند. **نکته کاربردی:** این الزام به گواهینامه‌هایی که توسط توابع امنیتی هدف ارزیابی استفاده و پردازش شده‌اند، اعمال می‌شود. گواهینامه‌هایی که توسط دیگر عناصر در محیط عملیاتی پردازش و استفاده شده‌اند، توسط این مؤلفه پوشش داده نمی‌شوند.
۴۸	**نام عنصر: گواهینامه‌های X509. ۱**

شماره	نام خانواده	عنصر امنیتی
الزام		

شماره مؤلفه: اش-X509 (ت‌س).۳,۱(FIA-X509-EXT.1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیتی را برای سرپرستان احراز هویت شده، ارائه دهند تا گواهینامه‌های X.509v3 جهت استفاده توسط توابع امنیتی مشخص شده در این پروفایل حفاظتی، در داخل هدف ارزیابی بارگذاری شوند.

۷,۵ کلاس مدیریت امنیت

هدف ارزیابی نیازی به نقش مدیریتی مجزا ندارد. با این حال نیاز است که قابلیتی ارائه شود تا جنبه‌های خاصی از هدف ارزیابی را که نباید در دسترس کاربر معمول قرار بگیرد پیکربندی کند. اگر هدف ارزیابی، سطحی از کنترل سرپرستی را ارائه دهد، بنابراین الزام مناسب توسط پیوست الف باید در هدف امنیتی استفاده شود.

نام کلاس: مدیریت امنیت

شرح کلاس: این کلاس جهت مشخص کردن مدیریت شاخصه‌های زیر در نظر گرفته شده است: مشخصه‌های امنیتی، توابع و داده‌های توابع امنیتی هدف ارزیابی. هم-چنین در این کلاس می‌توان نقش‌های مدیریتی مختلف، تعاملات آنها از جمله جداسازی قابلیت‌های هر نقش را مشخص نمود.
از اهداف این کلاس می‌توان به موارد زیر اشاره نمود:

- مدیریت داده توابع امنیتی هدف ارزیابی، برای مثال علامت‌ها[1]
- مدیریت مجوزهای امنیتی، برای مثال لیست‌های کنترل دسترسی و لیست قابلیت‌ها
- مدیریت عملکرد توابع امنیتی هدف ارزیابی برای مثال، انتخاب توابع ، نقش‌ها یا شرایطی که رفتار توابع امنیتی هدف ارزیابی را تحت تاثیر قرار می‌دهند.
- تعریف نقش‌های امنیتی

این کلاس دارای هفت خانواده است که هریک از آنها در ادامه شرح داده شده است.

➢ خانواده مدیریت کارکردها در توابع امنیتی هدف ارزیابی[2]

این خانواده به کاربران مجاز(نقش‌ها) اجازه می‌دهد تا بر روی مدیریت عملکردهای تعریف شده در هدف ارزیابی کنترل داشته باشند. مثالی از عملکردها در توابع امنیتی هدف ارزیابی، شامل ممیزی توابع و توابع احراز هویت چندگانه می‌باشد.

➢ خانواده مدیریت مشخصات امنیتی[3]

این خانواده به کاربران مجاز(نقش‌ها) اجازه می‌دهد تا بر روی مدیریت مشخصه‌های امنیتی کنترل داشته باشند. این مدیریت می‌تواند شامل قابلیتی برای مشاهده و تغییر مشخصات امنیتی باشد.

➢ خانواده مدیریت داده‌های توابع امنیتی هدف ارزیابی[4]

این خانواده به کاربران مجاز(نقش‌ها) اجازه می‌دهد تا بر روی مدیریت داده‌های توابع امنیتی هدف ارزیابی کنترل داشته باشند. مثالی از داده توابع امنیتی هدف ارزیابی می‌تواند شامل ممیزی اطلاعات، ساعت و دیگر پارامترهای پیکربندی توابع امنیتی هدف ارزیابی باشد.

---

1 Banner
2 Management of functions in TSF(FMT_MOF)
3 Management of security attributes(FMT_MSA)
4 Management of TSF data(FMT_MTD)

- **خانواده لغو[1]**

این خانواده لغو مجوزهای امنیتی انواع موجودیت‌ها را در هدف ارزیابی نشان می‌دهد.

- **خانواده انقضای ویژگی‌های امنیتی[2]**

این خانواده قادر به اعمال محدودیت زمانی برای اعتبار مجوزهای امنیتی می‌باشد.

- **خانواده مشخص نمودن عملکردهای مدیریتی[3]**

این خانواده اجازه می‌دهد تا عملکردهای مدیریتی ارائه شده توسط هدف ارزیابی مشخص شود. عملکردهای مدیریتی با فراهم نمودن رابط توابع امنیتی هدف ارزیابی[4]، به سرپرستان اجازه می‌دهند تا پارامترهایی را برای کنترل عملکرد ویژگی‌های مربوط به امنیت هدف ارزیابی تعریف کند، مانند مجوزها و صفات حفاظت از داده، مجوزها و صفات حفاظت از هدف ارزیابی، مجوزها و صفات ممیزی و مجوزها و صفات شناسایی و احراز هویت.
کارکردهای مدیریتی هم‌چنین شامل آن دسته از کارکردهایی است که توسط کاربر اجرا می‌شود تا تداوم کارکرد هدف ارزیابی را تضمین کند، مانند کارکردهای پشتیبانی و بازیابی. کارکرد این خانواده بر روی دیگر مؤلفه‌ها در کلاس مدیریت امنیت تاثیر دارد.

- **خانواده نقش‌های مدیریت امنیتی[5]**

این خانواده برای کنترل اختصاص نقش‌های مختلف به کاربران در نظرگرفته شده است. توانایی این نقش‌ها با توجه به مدیریت امنیتی است که در دیگر خانواده‌های این کلاس توصیف شده است.

---

1 Revocation(FMT_REV)
2 Security attribute expiration(FMT_SAE)
3 Specification of Management Functions (FMT_SMF)
4 TOE Security FunctionalityInterface (TSFI)
5 Security management roles (FMT_SMR)

هدف اصلی این بخش، اعلام خطر کردن در ارتباط با فعالیت‌های حساس است که باید توسط سرپرست انجام گیرد تا از غفلت کاربر در رابطه با قرارگیری سامانه دسترسی WLAN در یک حالت ناامن جلوگیری کند.چنانچه قابلیت‌های بیشتری توسط هدف ارزیابی ارائه شود، الزامات شناسایی و مدیریت مناسب توسط پیوست الف باید در هدف امنیتی در نظر گرفته شود.

شماره الزام	نام خانواده	عنصر امنیتی
۴۹	مدیریت رفتار توابع امنیتی (FMT_MOF)	**نام عنصر:** مدیریت رفتار توابع امنیتی ۱ **شماره مؤلفه: م‌د-م‌ت.۱،۱ (FMT_MOF.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قابلیت فعال سازی، غیر فعال سازی، تعیین و تغییر رفتار تمام توابع امنیتی هدف ارزیابی که در این پروفایل حفاظتی معرفی شده است را به سرپرست احراز هویت شده محدود کنند. **نکته کاربردی:** تنها کاربران انسانی هدف ارزیابی، کاربرانی هستند که نقش سرپرستی دارند؛ بنابراین، این الزام به کاربرانی

شماره الزام	نام خانواده	عنصر امنیتی
		غیر از سرپرست اشاره دارد که قادر نخواهند بود سازوکارهایی از هدف ارزیابی را که در پیاده‌سازی الزامات امنیتی پروفایل حفاظتی استفاده می‌شوند، دستکاری کنند. این قابلیت‌ها به صراحت توابع پیاده‌سازی شده در هدف ارزیابی را با توجه به اضافه شدن عناصر هدف ارزیابی که به شبکه اضافه شده‌اند پوشش می‌دهند و آنها را از دیدگاه افزونگی یا مدیریت ساخت یافته می‌کنند.
۵۰	مدیریت داده های توابع امنیتی هدف ارزیابی (**FMT_MTD**)	**نام عنصر: مدیریت داده های توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: م‌د-م‌د.۱,۱.۱ (FMT_MTD.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید توانایی **مدیریت** داده‌های توابع امنیتی هدف ارزیابی را تنها به سرپرست امنیتی محدود کند. **نکته کاربردی:** عبارت **"مدیریت"** می‌تواند شامل انجام موارد زیر باشد، اما تنها به این موارد نیز محدود نمی‌شود: • ایجاد، مقداردهی، مشاهده، تغییر پیش‌فرض، تغییردادن،حذف نمودن، پاک کردن و اضافه نمودن

شماره الزام	نام خانواده	عنصر امنیتی
		این الزام به طور پیش‌فرض برای مدیریت داده توابع امنیتی هدف ارزیابی درنظرگرفته می‌شود. به عنوان مثال داده‌های توابع امنیتی هدف ارزیابی می‌تواند شامل اطلاعات رمزنگاری باشد و هم‌چنین، مدیریت این داده‌ها شامل مرتبط کردن پروتکل رمزنگاری به واسط می‌باشد.
۵۱		**نام عنصر: مدیریت داده های توابع امنیتی هدف ارزیابی ۱(۲)**
		شماره مؤلفه: م‌د-م‌د.۱,۱(۲) ((FMT_MTD.1.1(2))
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید از خواندن داده‌های احراز هویت مبتنی بر رمزعبور جلوگیری کنند.
		نکته کاربردی:
		منظور این الزام آن است که هیچ کاربر یا سرپرستی قادر به خواندن داده احراز هویت اولیه (همانند رمزعبور رمز نشده) از طریق واسط‌های "معمولی" نمی‌باشد چنانچه خواندن چنین داده‌هایی منجر به جعل هویت کاربر شود. مدیر قدرتمند می‌تواند مستقیماً حافظه را بخواند یا با یک خواندن اولیه‌ی فایل سامانه رمز عبور را به دست آورد اما اعتمادی به انجام این کار نیست.

شماره الزام	نام خانواده	عنصر امنیتی
۵۲		**نام عنصر: مدیریت داده های توابع امنیتی هدف ارزیابی(خواندن تمام کلیدهای متقارن) ۱** **شماره مؤلفه: م‌د-م‌د.۱,۱.۱ (FMT_MTD.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از خواندن تمام کلیدهای از پیش به اشتراک گذاشته شده، کلید متقارن و کلیدهای خصوصی جلوگیری کند. **نکته کاربردی:** منظور این الزام آن است که هیچ کاربر یا سرپرستی قادر به خواندن یا مشاهده کلیدهای شناسایی شده (ذخیره شده یا موقتی) از طریق واسطهای "معمولی" می‌باشد. درحالیکه سرپرست مجاز می‌تواند با خواندن مستقیم حافظه این کلیدها را مشاهده کند، اما اعتمادی به انجام این کار نیست.
۵۳	خانواده مشخصات کارکردهای مدیریتی **(FMT_SMF)**	**نام عنصر:** مشخصات کارکردهای مدیریتی **۱** **شماره مؤلفه: م‌د-ع‌م.۱,۱.۱ (FMT_SMF.1.1)** **شرح مؤلفه:**

شماره الزام	نام خانواده	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید توانایی اجرای کارکردهای مدیریتی زیر را داشته باشد:

- توانایی در پیکربندی لیست سرویس‌های هدف ارزیابی که پیش از شناسایی و احراز هویت همان-طور که در عنصر اش-ش‌ه.۱ در دسترس می‌باشند.
- توانایی پیکربندی عملکرد رمزنگاری
- توانایی به روزرسانی هدف ارزیابی، و بررسی به روزرسانی‌ها با استفاده از قابلیت امضاء دیجیتال (رز-ع‌ر.۱(۲)) و [انتخاب: بدون هیچ عملکرد دیگر، [اختصاص: دیگر عملکردهای (یا دیگر عملکردها) که در پشتیبانی قابلیت به روزرسانی استفاده شده است]].
- توانایی پیکربندی تذکرات راهنما و پیغام‌های هشدار توافقی با توجه به استفاده غیرمجاز از هدف ارزیابی.
- توانایی پیکربندی تمام عملکردهای مدیریت امنیتی که در دیگر بخش‌های این پروفایل حفاظتی معرفی شده است.

نکته کاربردی:

شماره الزام	نام خانواده	عنصر امنیتی
		عملکردهای مدیریت امنیتی برای عنصر مد-ع‌م.۱ از طریق این پروفایل حفاظتی توزیع شده است و به عنوان بخشی از الزامات در عنصرهای مد-مت، مد-ما، مد-مد، مد-ل‌غ و هر تابع مدیریتی رمزنگاری که در استاندارد مرجع مشخص شده است، در نظر گرفته می‌شود
۵۴		**نام عنصر:** مشخصات کارکردهای مدیریتی **۱** **شماره مؤلفه: مد-ن‌م.۱،۱ (FMT_SMR.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید نقش‌های زیر را نگهداری کنند: • سرپرست مجاز • [هیچ نقش دیگر]
	نقش‌های مدیریت امنیت **(FMT_SMR)**	
۵۵		**نام عنصر:** مشخصات کارکردهای مدیریتی **۱** **شماره مؤلفه: مد-ن‌م.۲،۱ (FMT_SMR.1.2)** **شرح مؤلفه:**

شماره الزام	نام خانواده	عنصر امنیتی

توابع امنیتی هدف ارزیابی باید قادر باشد کاربران را به نقش‌هایشان مرتبط کند.

نکته کاربردی:

مؤلفه م‌د-ع‌م.۲,۱ ملزم می‌کند که حساب کاربری تنها به یک نقش مرتبط شود. هرچند که چندین کاربر ممکن است نقش مشابهی را داشته باشند و هدف ارزیابی نیازی به محدود کردن نقش‌ها به یک فرد خاص ندارد.

۵۶ **نام عنصر:** مشخصات کارکردهای مدیریتی **۱**

شماره مؤلفه: م‌د-ن‌م.۳,۱ (FMT_SMR.1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد که شرایط زیر برآورده می‌شود:

- نقش سرپرست مجاز باید قادر به سرپرستی هدف ارزیابی به صورت محلی باشد.
- نقش سرپرست مجاز باید قادر به سرپرستی هدف ارزیابی به صورت از راه دور باشد.
- توانایی سرپرستی از راه دور هدف ارزیابی از یک کلاینت بی‌سیم باید به صورت پیش‌فرض غیرفعال

شماره الزام	نام خانواده	عنصر امنیتی

باشد.

نکته کاربردی:

مؤلفه مد-ع‌م.۳,۱ ملزم می کند که سرپرست مجاز قادر به سرپرستی هدف ارزیابی از طریق کنسول محلی و از طریق یک سازوکار از راه دور می‌باشد (IPsec، SSH، TLS/HTTPS).

۷,۶ کلاس حفاظت از توابع امنیتی هدف ارزیابی

نام کلاس: حفاظت از توابع امنیتی هدف ارزیابی

شرح کلاس:

این کلاس در برگیرنده خانواده‌هایی در ارتباط با صحت و مدیریت سازوکارهای تشکیل دهنده‌ی توابع امنیتی هدف ارزیابی و صحت داده توابع امنیتی هدف ارزیابی می-باشند. از بعضی جهات، خانواده‌های این کلاس ممکن است به نظر بیاید که تکرار عناصر کلاس محافظت از داده کاربری است، حتی ممکن است هر دوی این کلاس‌ها با سازوکار مشابهی پیاده‌سازی شده‌باشد. هرچند کلاس محافظت از داده کاربری بر روی محافظت از داده کاربر متمرکز شده است اما کلاس محافظت از توابع امنیتی هدف

ارزیابی بر روی محافظت از داده‌های توابع امنیتی هدف ارزیابی متمرکز شده است. در حقیقت، عناصر کلاس محافظت از توابع امنیتی هدف ارزیابی لازم است الزاماتی را ارائه کنند تا خط‌مشی‌های عملکرد امنیتی در هدف ارزیابی نتوانند مورد مداخله قرار بگیرند یا دور زده[1] شوند.

از دیدگاه این کلاس، باتوجه به توابع امنیتی هدف ارزیابی سه مؤلفه مهم وجود دارد:

- پیاده‌سازی توابع امنیتی هدف ارزیابی، که سازوکارهای اجرا کننده توابع امنیتی هدف ارزیابی را اجرا و پیاده‌سازی می‌کند.
- داده توابع امنیتی هدف ارزیابی، که پایگاه داده‌های سرپرستی، راهنمایی کننده‌ی اجرای عملکرد امنیتی می‌باشند.
- موجودیت‌های خارجی که توابع امنیتی هدف ارزیابی، ممکن است جهت اجرای الزامات عملکرد امنیتی با آنها در تعامل باشند.

➢ خانواده شکست امن[2]

الزامات این خانواده اطمینان می‌دهد هنگامی که مجموعه‌ای از شکست‌های مشخص در توابع امنیتی هدف ارزیابی روی می‌دهد، هدف ارزیابی الزامات عملکرد امنیتی (کارکرد امنیتی لازم) را اجرا می‌کند. این خانواده تنها یک عنصر دارد که ملزم می کند در زمان رخ دادن شکست، عملکرد امنیتی هدف ارزیابی در وضعیت امن نگهداشته شود.

➢ خانواده دسترس‌پذیری داده ارسال شده توابع امنیتی هدف ارزیابی[3]

این خانواده قوانینی را تعریف می‌کند که در هنگام انتقال داده توابع امنیتی هدف ارزیابی بین توابع امنیتی هدف ارزیابی و دیگر محصولات IT از نبود دسترسی به این داده‌ها، جلوگیری می‌کند. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی، یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشند.

---

1 Bypass

2 Fail secure(FPT_FLS)

3 Availability of exported TSF data(FPT_ITA)

- **خانواده محرمانگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[1]**

این خانواده تعریف کننده‌ی قوانینی برای محافظت از افشای غیرمجاز داده توابع امنیتی هدف ارزیابی در طول انتقال بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT می‌باشد. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی، یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده یکپارچگی داده‌های ارسال شده توابع امنیتی هدف ارزیابی[2]**

این خانواده تعریف کننده قوانینی برای حفاظت از تغییرات غیرمجاز داده‌های توابع امنیتی هدف ارزیابی است که بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT منتقل می‌شوند. برای مثال این داده می‌تواند، داده‌های حساس توابع امنیتی هدف ارزیابی هم‌چون رمز عبور، کلیدها، داده ممیزی، یا کدهای اجرایی توابع امنیتی هدف ارزیابی باشد.

- **خانواده انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی[3]**

این خانواده الزاماتی را ارائه می کند که از داده توابع امنیتی هدف ارزیابی در زمان انتقال بین بخش‌های مجزای توابع امنیتی هدف ارزیابی در سراسر کانال داخلی محافظت می‌کند.

- **خانواده محافظت فیزیکی از توابع امنیتی هدف ارزیابی[4]**

مؤلفه‌های حفاظت فیزیکی توابع امنیتی هدف ارزیابی به محدودیت‌هایی بر روی دستیابی فیزیکی غیرمجاز به توابع امنیتی هدف ارزیابی، بازدارندگی از، مقاومت در برابر، اصلاح فیزیکی غیرمجاز یا جایگزینی توابع امنیتی هدف ارزیابی اشاره دارند.

---

1 Confidentiality of exported TSF data (FPT_ITC)

2 Integrity of exported TSF data (FPT_ITI)

3 Internal TOE TSF data transfer (FPT_ITT)

4 TSF physical protection (FPT_PHP)

الزامات مؤلفه‌ها در این خانواده این اطمینان را می‌دهند که از توابع امنیتی هدف ارزیابی در برابر مداخله فیزیکی و تداخلات محافظت می‌شود. برآورده شدن این مؤلفه‌ها منجر به بسته‌بندی و استفاده توابع امنیتی هدف ارزیابی به صورتی می‌شود که مداخلات فیزیکی قابل تشخیص باشند و یا مجبور به مقاومت در برابر تداخلات فیزیکی شوند. بدون این مؤلفه‌ها، عملکرد حفاظتی از توابع امنیتی هدف ارزیابی اثرشان را در محیط‌هایی که از آسیب فیزیکی نمی‌توان جلوگیری کرد، از دست می‌دهند این خانواده هم‌چنین الزاماتی را ارائه داده است که چطور توابع امنیتی هدف ارزیابی باید به تلاش‌هایی که در ارتباط با تداخل فیزیکی صورت می‌گیرد واکنش نشان دهند.

- **خانواده بازیابی مطمئن[1]**

الزامات این خانواده توابع امنیتی هدف ارزیابی را ملزم می‌کند تا بعد از رخ دادن شکست یا قطع عملیات، هدف ارزیابی در یک وضعیت امن باقی بماند و بدون به خطر افتادن حفاظتش بازیابی و راه‌اندازی شود. این خانواده بسیار مهم است زیرا وضعیت راه‌اندازی توابع امنیتی هدف ارزیابی، تعیین کننده‌ی حفاظت از وضعیت‌های بعدی می‌باشد.

- **خانواده تشخیص تکرار[2]**

در این خانواده توابع امنیتی هدف ارزیابی ملزم به تشخیص تکرار انواع موجودیت‌ها (به طور مثال، پیغام‌ها، درخواست‌های سرویس، پاسخ‌های سرویس) مشخص شده در الزام می‌باشند؛ هم‌چنین در زمان تشخیص تکرار، توابع امنیتی هدف ارزیابی باید اقدام خاصی را انجام بدهند.

- **خانواده پروتکل هم‌زمانی حالت[3]**

هدف ارزیابی توزیع شده ممکن است نسبت به هدف ارزیابی واحد، به واسطه‌ی اختلاف حالت‌ها بین بخش‌های مختلف هدف ارزیابی و تاخیر در ارتباطات دارای پیچیدگی بیشتر باشد. در اغلب موارد هم‌زمان‌سازی حالت‌ها بین عملکردهای توزیع یافته مستلزم یک پروتکل تبادلی است و یک عمل ساده نیست.
در حالتی که عدم اعتماد به محیط توزیع وجود داشته باشد، به پروتکل هم‌زمان‌سازی پیچیده‌تری نیاز است.

---

1 Trusted recovery (FPT_RCV)

2 Replay detection (FPT_RPL)

3 State synchrony protocol (FPT_SSP)

پروتکل هم‌زمان‌سازی، الزاماتی را برای عملکردهای بحرانی مربوط به تابع امنیتی هدف ارزیابی ایجاد می‌کند تا از این پروتکل امن استفاده کنند. پروتکل هم‌زمان‌سازی اطمینان می‌دهد که دو بخش توزیعی هدف ارزیابی (به طور مثال، میزبان‌ها) حالت‌هایشان را بعد از اقدامات مرتبط امنیتی هم‌زمان می‌کنند.

- **خانواده مهرهای زمانی[1]**

این خانواده، الزاماتی را برای یک مهر زمانی معتبر در داخل هدف ارزیابی، نشان می‌دهد.

- **خانواده هم‌خوانی داده‌های بین توابع امنیتی هدف ارزیابی[2]**

در یک محیط توزیعی، هدف ارزیابی ممکن است به تبادل داده توابع امنیتی هدف ارزیابی با دیگر محصولات امن IT نیاز داشته باشد. این خانواده الزاماتی را برای به اشتراک گذاری و تفسیر سازگار مجوزها، بین توابع امنیتی هدف ارزیابی مربوط به هدف ارزیابی و یک محصول امن IT متفاوت تعریف می‌کند.

- **خانواده آزمون موجودیت‌های خارجی[3]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف می کند تا آزمون‌هایی را بر روی یک یا بیش از یک موجودیت خارجی انجام دهند. عناصر مطرح شده در این خانواده برای اعمال به کاربران انسانی در نظر گرفته نشده‌اند.

موجودیت‌های خارجی، ممکن است شامل برنامه‌هایی باشند که بر روی هدف ارزیابی اجرا می‌شوند، سخت‌افزار و نرم‌افزاری که تحت هدف ارزیابی اجرا می‌شود(پلتفرم‌ها، سامانه‌عامل و ...) یا برنامه‌ها و باکس‌های متصل شده به هدف ارزیابی (سامانه‌های تشخیص نفوذ، فایروال‌ها، سرورهای ورود، سرورهای زمانی و غیره) باشد.

1 Time stamps (FPT_STM)

2 Inter-TSF TSF data consistency

3 Testing of external entities(FPT_TEE)

- **خانواده هم‌خوانی تکرار داده‌ها در توابع امنیتی هدف ارزیابی در داخل هدف ارزیابی[1]**

الزامات این خانواده از آن جهت لازم و ضروری می‌باشد، تا از هم‌خوانی داده توابع امنیتی هدف ارزیابی زمانی‌که در داخل هدف ارزیابی تکرار می‌شود، اطمینان حاصل کند. منظور از هم‌خوانی داده‌ها، یکسان بودن داده‌ها در محلها و توابع مختلف است. داده‌ی توابع امنیتی هدف ارزیابی زمانی ناهم‌خوان می‌شود که کانال داخلی بین بخش‌های مختلف هدف ارزیابی نامعتبر شود. اگر اجزای هدف ارزیابی از نظر داخلی تشکیل یک شبکه بدهند، در صورت غیر فعال شدن ارتباطات شبکه‌ای، عدم هم‌خوانی بین داده-های تابع امنیتی می‌تواند رخ دهد.

- **خانواده خودآزمایی توابع امنیتی هدف ارزیابی[2]**

این خانواده الزاماتی را برای خودآزمایی توابع امنیتی هدف ارزیابی با توجه به عملکرد صحیح مورد انتظار تعریف می‌کند. اجبار هدف ارزیابی به انجام آزمون بر روی بخشهای حساس و مهم هدف ارزیابی با استفاده از نمونه عملیات‌های ریاضی مثالی از این الزام می باشد. این‌گونه آزمون‌ها می‌توانند در هنگام راه اندازی، به طور متناوب بنا به درخواست کاربر مجاز، یا در زمانی‌که شرایط خاصی ایجاد شود، انجام گیرد. عملی که باید به عنوان نتیجه خودآزمایی توسط هدف ارزیابی انجام شود در دیگر خانواده‌ها تعریف می‌شود.

الزامات این خانواده هم‌چنین برای تشخیص عدم صحت داده‌ی توابع امنیتی هدف ارزیابی و یا خود توابع امنیتی هدف ارزیابی (کد اجرایی یا مؤلفه‌های سخت‌افزاری توابع امنیتی هدف ارزیابی) توسط خرابی‌های مختلفی که لزوماً عملکرد هدف ارزیابی (که توسط دیگر خانواده‌ها اداره شده‌اند)را متوقف نمی‌کنند، مورد نیاز است.

چنین خرابی هایی می‌تواند یا به دلیل حالت‌های پیش‌بینی نشده خرابی یا سهل‌انگاری‌های مرتبط با طراحی سخت‌افزار، میان‌افزار یا نرم افزار رخ دهد و یا به دلیل تغییر مخرب توابع امنیتی هدف ارزیابی بر اثر حفاظت منطقی و/یا فیزیکی ناکافی صورت گیرد.

شماره	نام خانواده	عنصر امنیتی
الزام		

1 Internal TOE TSF data replication consistency(FPT_TRC)

2 TSF self test(FPT_TST)

شماره	نام خانواده	عنصر امنیتی
الزام		
۵۷	نقض امنیت (**FPT_FLS**)	**نام عنصر: نقض امنیت ۱** **شماره مؤلفه: ح‌ت-ن‌ا.۱،۱ (FPT_FLS.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید زمانی‌که انواع شکست‌های زیر رخ می‌دهد، وضعیت امنی را حفظ کنند: • شکست درخودآزمایی های راه‌اندازی. **نکته کاربردی:** این الزام بدان معناست که هدف ارزیابی باید زمانی‌که شکست شناخته شده‌ای رخ می‌دهد به یک وضعیت امنی دست پیدا کند. چنان‌چه هدف ارزیابی در اواسط یک عملیات بحرانی با شکست مواجه شد.
۵۸	شناسایی مجدد (**FPT_RPL**)	**نام عنصر: شناسایی مجدد ۱** **شماره مؤلفه: ح‌ت-ش‌م.۱،۱ (FPT_RPL.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تکرار شدن برای موجودیت‌های [بسته‌های شبکه منتقل شده در هدف

شماره	نام خانواده الزام	عنصر امنیتی
		ارزیابی] شناسایی کند.
۵۹		**نام عنصر: شناسایی مجدد ۱**
		شماره مؤلفه: ح‌ت-ش‌م.۲,۱ (FPT_RPL.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید زمانی‌که تکراری تشخیص داده شد: [داده را رد کنند].
		نکته کاربردی:
		دریافت بسته‌های شبکه‌های متعدد با توجه به تراکم شبکه یا اعلام دریافت بسته‌های از دست رفته به عنوان یک حمله تکرار در نظر گرفته نمی‌شود. منظور این الزام آن است که اطمینان داده شود که هر ارتباط با ماهیت امن (سرپرست به هدف ارزیابی، موجودیت IT به هدف ارزیابی، هدف ارزیابی به هدف ارزیابی) توسط مؤلفه پوشش داده می‌شود و نمی‌تواند تکرار شود.
۶۰	مهرهای زمانی (FPT_STM)	**نام عنصر: مهرهای زمانی ۱**
		شماره مؤلفه: ح‌ت-م‌ز.۱,۱ (FPT_STM.1.1)

شماره	نام خانواده	عنصر امنیتی	الزام

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قادر باشند برای استفاده خودشان مهرهای زمانی قابل اطمینانی ارائه دهند.

۶۱ خودآزمایی توابع امنیتی هدف ارزیابی (**FPT_TST**)

نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی ۱

شماره مؤلفه: حت-خا.(ت‌س).۱,۱.۱ (FPT_TST_EXT.1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید یک مجموعه خودآزمایی در طول راه‌اندازی اولیه اجرا کند تا عملکرد صحیح توابع امنیتی هدف ارزیابی را نشان دهند.

۶۲

عنصر: خودآزمایی توابع امنیتی هدف ارزیابی ۱

شماره مؤلفه: حت-خا.(ت‌س).۲,۱.۲ (FPT_TST_EXT.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیتی را ارائه دهد، تا یکپارچگی و صحت کد اجرایی ذخیره شده توابع امنیتی هدف ارزیابی در زمان بارگذاری برای اجرا از طریق استفاده از سرویس‌های رمزنگاری ارائه شده برای

شماره	نام خانواده	عنصر امنیتی
الزام		
		توابع امنیتی هدف ارزیابی که در عنصر رز-ع‌ر.۱(۲) مشخص شده است، بررسی و راستی آزمایی شوند.
۶۳	به روز رسانی امن (FPT_TUD)	**نام عنصر: به روز رسانی امن ۱** **شماره مؤلفه:** حت-رم-(ت س)۱,۱ **(FPT_TUD_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به مدیران مجاز این قابلیت را بدهند تا بتوانند نسخه فعلی نرم افزار/میان افزار هدف ارزیابی را پرس و جو و مشاهده کنند.
۶۴		**نام عنصر: به روز رسانی امن ۱** **شماره مؤلفه:** حت-رم-(ت س)۲,۱ **(FPT_TUD_EXT.1.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به مدیران مجاز این قابلیت را بدهند تا بتوانند فرآیند به روز رسانی نرم افزار/میان افزار هدف ارزیابی را انجام دهند.
۶۵		**نام عنصر: به روز رسانی امن ۱**

شماره نام خانواده

الزام

عنصر امنیتی

شماره مؤلفه: حت-رم-(ت س)۳,۱ **(FPT_TUD_EXT.1.3)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید به وسیله روشی قبل از به روز رسانی نرم‌افزار/میان‌افزار، با استفاده از سازوکارهای امضای دیجیتال،[انتخاب: مقادیر درهم‌سازی منتشر شده، هیچ عملکرد دیگر] از صحت به‌روز-رسانی نرم افزاری/میان افزاری پیش از نصب اطمینان حاصل کنند.

نکته کاربردی:

سازوکار امضاء دیجیتال اشاره به سومین الزام در عنصر رز-ع ر.۱(۲) دارد.

درهم‌سازی منتشرشده توسط یکی از توابع مشخص شده در رز-ع ر.۱(۳) تولید می‌شود.

۷,۷ کلاس دسترسی به هدف ارزیابی

نام کلاس: دسترسی به هدف ارزیابی

شرح کلاس: این خانواده الزامات عملیاتی برای کنترل نشست‌های کاربری برقرار شده را مشخص می‌کند.

- **خانواده محدودیت دامنه‌ی ویژگی‌های قابل انتخاب**[1]

این خانواده الزاماتی را تعریف می کند تا دامنه‌ی صفات و ویژگی‌های امنیتی نشست را که کاربری ممکن است برای نشست انتخاب کند محدود کند.

- **خانواده محدودیت برای نشست‌های هم‌زمان چندگانه**[2]

این خانواده الزاماتی را تعریف می‌کند که تعداد نشست‌های هم‌زمان را که متعلق به یک کاربر است محدود کند.

- **قفل کردن و خاتمه دادن نشست**[3]

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف کرده است تا قابلیتی را برای قفل کردن، باز کردن و خاتمه نشست‌های تعاملی که توسط توابع امنیتی هدف ارزیابی و کاربر آغاز شده است تعریف کند.

- **علائم دسترسی هدف ارزیابی**[4]

این خانواده تعریف کننده الزاماتی است تا یک پیغام هشدار مشورتی قابل تنظیم را به کاربران با توجه به استفاده مناسب از هدف ارزیابی نمایش دهد.

---

1 Limitation on scope of selectable attributes(FTA_LSA)

2 Limitation on multiple concurrent sessions(FTA_MCS)

3 Session locking and termination(FTA_SSL)

4 TOE access banners(FTA_TAB)

- **سوابق دسترسی به هدف ارزیابی[1]**

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف کرده است تا برای نشست‌هایی که موفقیت آمیز برقرار شده است، تاریخچه تلاش‌های موفق و ناموفق دستیابی به حساب کاربری را به کاربر نمایش دهد.

- **برقراری نشست هدف ارزیابی[2]**

این خانواده الزاماتی را تعریف می کند تا مجوز کاربری را جهت برقراری یک نشست با هدف ارزیابی انکار کند.

شماره الزام	نام خانواده	عنصر امنیتی
۶۶	قفل کردن و خاتمه دادن نشست (FTA_SSL)	**نام عنصر: قفل کردن و پایان دادن به نشست‌های شروع شده توسط توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه: دس-ق‌ن-(ت‌س).۱,۱(FTA_SSL_EXT.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پس از یک مدت زمان مشخص غیرفعال بودن، برای نشست‌های تعاملی محلی [انتخاب:

1 TOE access history(FTA_TAH)

2 TOE session establishment(FTA_TSE)

شماره نام خانواده

الزام

عنصر امنیتی

۱. قفل کردن نشست، پاک کردن یا رونویسی صفحه نمایش دستگاه که سبب می‌شود محتوای فعلی غیرقابل خواندن شود، غیرفعال‌سازی کلیه فعالیت‌های مربوط به دسترسی داده‌های کاربر و دستگاه‌های نمایش. همچنین نیاز است که پیش از باز شدن نشست، توابع امنیتی هدف ارزیابی، سرپرست را دوباره احراز هویت کند

۲. خاتمه دادن نشست] .

مدت زمان مشخص غیرفعال بودن، توسط سرپرست تعیین شود.

۶۷ **نام عنصر:** قفل گذاری بر روی نشست ها و خاتمه دادن به آنها **۳**

شماره مؤلفه: دس-ق‌ن.۱,۳(FTA_SSL.3.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید نشست تعاملی راه دور [1]را پس از مدت زمان مشخص غیرفعال بودن، خاتمه دهد.

1 remote

شماره الزام	نام خانواده	عنصر امنیتی
		مدت زمان مشخص غیرفعال بودن، توسط سرپرست تعیین شود.
۶۸		**نام عنصر:** قفل گذاری بر روی نشست ها و خاتمه دادن به آنها **۴** **شماره مؤلفه: دس-ق‌ن.۱,۴(FTA_SSL.4.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به شروع کننده نشست، اجازه اتمام نشست تعاملی خودش را بدهند.
۶۹	علائم دسترسی هدف ارزیابی **(FTA_TAB)**	**نام عنصر: علایم پیش‌فرض دسترسی هدف ارزیابی ۱** **شماره مؤلفه: دس-ع‌د.۱,۱ (FTA_TAB.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پیش از آغاز نشست کاربری، پیام هشداری مختص به سرپرست مجاز را که بیانگر استفاده مجاز از هدف ارزیابی است نمایش دهند. **نکته کاربردی:** این الزام به نشست‌های تعاملی بین کاربر انسانی و هدف ارزیابی اعمال می‌شود. موجودیت‌های IT اتصالات

شماره	نام خانواده	عنصر امنیتی
الزام		
		یا اتصالات برنامه‌ریزی شده‌ای (رویه‌های راه دوری که بر روی یک شبکه فراخوانی می‌شوند) را برقرار می-کند که لازم نیست توسط این الزام پوشش داده شود.
۷۰	ایجاد نشست هدف ارزیابی (FTA_TSE)	**نام عنصر:** ایجاد نشست هدف ارزیابی **۱** **شماره مؤلفه: دس-ان.۱،۱ (FTA_TSE. 1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید قادر باشند برقراری یک نشست کلاینت راه دور را با توجه به موقعیت، زمان، روز، [اختصاص: دیگر ویژگی‌ها] رد کند. **نکته کاربردی:** «موقعیت» می‌تواند به صورت یک شماره پورت، آدرس IP، زیرشبکه، VLAN، واسط هدف ارزیابی و ... مشخص شود. قسمت «اختصاص» توسط نویسنده هدف امنیتی استفاده می‌شود تا ویژگی‌های بیشتری که نشست‌های برقرار شده می‌توانند براساس آنها انکار شوند را مشخص کند.

۷,۸ کلاس تخصیص منابع

نام کلاس: تخصیص منابع

شرح کلاس: این کلاس ارائه کننده سه خانواده است که از دسترس پذیری منابع لازم هم‌چون قابلیت پردازش و/ یا ظرفیت ذخیره‌سازی پشتیبانی می‌کند. خانواده تحمل خرابی، ارائه کننده حفاظت درقبال قابلیت‌های ناشی از شکست هدف ارزیابی می‌باشد. خانواده اولویت سرویس اطمینان خواهد داد که منابع به فعالیت‌های خیلی مهم یا زمان بحرانی تخصیص داده می‌شود و فعالیت‌های با اولویت پائین‌تر نمی‌توانند این سرویس‌ها را به انحصار خود درآورند. خانواده تخصیص منابع، محدودیت‌هایی را بر روی استفاده از منابع در دسترس اعمال می‌کند، بنابراین از انحصار منابع توسط کاربران جلوگیری می کند.

- **خانواده تحمل خرابی**

الزامات این خانواده اطمینان می‌دهد که هدف ارزیابی حتی در زمان رویدادن یک رخداد شکست، از عملکرد صحیحش نگهداری خواهد نمود.

- **خانواده اولویت سرویس**

الزامات این خانواده به توابع امنیتی هدف ارزیابی اجازه می‌دهد تا استفاده از منابع تحت کنترل توابع امنیتی هدف ارزیابی را توسط کاربران و موجودیت‌های فعالی کنترل کند، به گونه‌ای که فعالیت‌های با اولویت بالا تحت کنترل توابع امنیتی هدف ارزیابی همواره بدون مداخله‌های غیرضروری یا تاخیر ناشی از فعالیت‌های با اولویت پایین انجام می‌شوند.

- **خانواده تخصیص منابع**

الزامات این خانواده به توابع امنیتی هدف ارزیابی اجازه می‌دهد تا استفاده از منابع را توسط کاربران و موجودیت‌های فعال کنترل کند، به طوریکه انکار سرویس به دلیل

انحصارگرایی غیرمجاز منابع رخ نخواهد داد.

شماره	نام خانواده الزام	عنصر امنیتی
۷۱	تخصیص منابع (FRU_RSA)	**نام عنصر:حداکثر طرفیت ۱** **شماره مؤلفه: م‌ن-ت‌م.۱,۱ (FRU_RSA.1.1)**

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید حداکثر ظرفیت منابع زیر را به اجرا درآورد:

[اختصاص: منابعی که واسطهای سرپرستی را پشتیبانی می کنند]، [انتخاب: [اختصاص: منابع کنترل شده]، هیچ منبع دیگر] که [انتخاب: کاربران فردی، گروهی از کاربران تعریف شده، موجودیت‌های فعال]می‌توانند از آنها [انتخاب: هم‌زمان، در یک بازه زمانی مشخص] استفاده کنند.

نکته کاربردی:

حداقل، هدف‌های ارزیابی منطبق براین پروفایل حفاظتی، باید حداکثر ظرفیت را بر روی منابع فراگیری که در پشتیبانی واسطهای سرپرستی راه دور استفاده می‌شوند اعمال کنند. این منابع در اولین «اختصاص» لیست می‌شوند. منابع دیگری که می‌تواند کنترل شود، باید در دومین «اختصاص» لیست شود. در صورتی-

شماره	نام خانواده	عنصر امنیتی	الزام
			که هیچ منبعی وجود نداشته باشد، آخرین آیتم در این قسمت باید انتخاب شود. دومین انتخاب باید مصرف کنندگان منابع کنترل شده را منعکس کند. آخرین انتخاب به منظور محدود نمودن بازه زمانی در ارتباط با استفاده از منابع کنترل شده استفاده می‌شود (به طور مثال، حداکثر طرفیتی اتصال TCP که از یک آدرس IP در مدت ۳۰ ثانیه درخواست می‌شود).

۷,۹ کلاس کانال/مسیر امن

نام کلاس: کانال‌ها و مسیرهای مورد اعتماد

شرح کلاس: خانواده‌های این کلاس الزاماتی را برای یک مسیر ارتباطی امن بین کاربران و توابع امنیتی هدف ارزیابی تعریف کرده‌اند، هم‌چنین الزاماتی را برای یک کانال ارتباطی امن بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT ارائه کرده‌اند. مسیر و کانال امن دارای شاخصه‌های اصلی زیر هستند:

- مسیر ارتباطی از کانال‌های ارتباطی داخلی و خارجی ساخته شده است که زیر مجموعه مشخصی از داده توابع امنیتی هدف ارزیابی و فرامین را از باقی توابع امنیتی هدف ارزیابی و داده کاربر جداسازی می‌کند.
- استفاده از مسیر ارتباطی ممکن توسط کاربر و یا توابع امنیتی هدف ارزیابی آغاز شود.
- مسیر ارتباطی می‌تواند اطمینان دهد که کاربر با توابع امنیتی هدف ارزیابی به طور صحیح در ارتباط است و اینکه توابع امنیتی هدف ارزیابی با کاربر به طور صحیح در ارتباط است.

در این نمونه، یک کانال امن، کانال ارتباطی است که ممکن است از هر دو سوی کانال راه‌اندازی شود و ارائه دهنده‌ی شاخصه‌ی غیرقابل انکار بودن با توجه به هویت آن سمت از کانال است.
یک مسیر امن، ارائه دهنده قابلیتی برای کاربران است تا فعالیتشان را از طریق یک تعامل مستقیم و مطمئن یا توابع امنیتی هدف ارزیابی انجام دهند. مسیر امن غالباً برای اقدامات کاربر هم‌چون شناسایی و احراز هویت اولیه مطلوب است، اما ممکن است در زمان‌های دیگری در طول بازه زمانی یک نشست کاربری نیز مفید باشد و تبادلات مسیر امن ممکن است توسط کاربر یا توابع امنیتی هدف ارزیابی آغاز شود. پاسخ امن از طریق مسیر امن تضمین می‌کند که از تغییرات توسط برنامه ناامن یا افشاء شدن برای یک برنامه ناامن محافظت می‌کند.

- **کانال مورد اعتماد بین توابع امنیتی هدف ارزیابی[1]**

این خانواده تعریف کننده الزاماتی برای ایجاد یک کانال ارتباطی امن بین توابع امنیتی هدف ارزیابی و دیگر محصولات امن IT است تا عملکردهای حساس امنیتی کارایی لازم را داشته باشد. این خانواده باید هنگامی‌که الزاماتی برای ارتباط امن کاربر یا داده توابع امنیتی هدف ارزیابی بین هدف ارزیابی و دیگر محصولات امن IT وجود دارد، در نظر گرفته شود.

- **مسیر مورداعتماد[2]**

این خانواده تعریف کننده الزاماتی برای برقراری و نگهداری ارتباط امن به/از کاربران و توابع امنیتی هدف ارزیابی است. یک مسیر امن ممکن است برای هر تعامل مرتبط امنیتی لازم باشد. تبادلات مسیر امن ممکن است توسط کاربر در طول تعامل با توابع امنیتی هدف ارزیابی آغاز شود، یا توابع امنیتی هدف ارزیابی ممکن است از طریق مسیر امن، ارتباطی را با کاربر برقرار کنند.

1 Inter-TSF trusted channel(FTP_ITC)

2 Trusted path(FTP_TRP)

شماره الزام	نام خانواده	عنصر امنیتی
۷۲	کانال مورداعتماد بین توابع امنیتی هدف ارزیابی **(FTP_ITC)**	**نام عنصر: کانال مورداعتماد داخلی توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه:** مم-ک‌م.۱,۱ (FTP_ITC.1.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید با استفاده از 802.11-2007، 802.1X و IPsec، و[انتخاب:SSH،TLS، TLS/HTTPS، هیچ پروتکل دیگر] کانال ارتباطی امنی بین خود و تمام موجودیت‌های مجاز IT ارائه کند که به طور منطقی از دیگر کانال‌های ارتباطی جدا است و به صورت مطمئن نقطه پایانی‌اش را شناسایی می‌کند و از داده‌های کانال در برابر تغییر یا افشاء، محافظت می‌کند.
۷۳		**نام عنصر: کانال مورداعتماد داخلی توابع امنیتی هدف ارزیابی ۱** **شماره مؤلفه:** مم-ک‌م.۲,۱ (FTP_ITC.1.2) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید اجازه شروع ارتباط از طریق کانال مورد اعتماد را به خود و موجودیت‌های IT مجاز بدهند.

شماره الزام	نام خانواده
۷۴	عنصر امنیتی

نام عنصر: کانال مورداعتماد داخلی توابع امنیتی هدف ارزیابی ۱

شماره مؤلفه: مم-ک‌م.۳,۱ (FTP_ITC.1.3)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید ارتباطات را از طریق کانال مورداعتماد برای [اختصاص: لیستی از سرویس‌هایی که توابع امنیتی هدف ارزیابی قادر به راه اندازی ارتباط‌هایشان است] شروع کنند.

نکته کاربردی:

منظور الزام بالا استفاده از پروتکل رمزنگاری معرفی شده، جهت محافظت از تمام ارتباطات خارجی هدف ارزیابی با موجودیت IT مجاز، می‌باشد. استاندارد 802.11-2007 برای ارتباط با کلاینت‌های وایرلس لازم است.

پروتکل IPsec حداقل برای ارتباط با سرور احراز هویت لازم و ضروری است. اگر نیاز به ارتباط با دیگر موجودیت‌های IT مجاز باشد(سرور NTP، سرور ممیزی)، بنابراین نویسنده هدف امنیتی باید از پروتکل IPsec یا یکی دیگر از پروتکل‌های لیست شده استفاده کند(پروتکل SSH، TLSو TLS/HTTPS که مجاز

شماره نام خانواده

الزام

عنصر امنیتی

هستند)، و بنابراین انتخاب مناسبی داشته باشد. پس از آنکه نویسنده هدف امنیتی یکی از پروتکل‌ها را انتخاب نمود، آنها باید در قسمت پیوست C الزاماتی جزئی‌تری را متناسب با انتخابشان در هدف امنیتی قرار دهند.

درحالی‌که هیچ الزامی بر روی بخش راه‌اندازی ارتباط وجود ندارد، نویسنده هدف امنیتی در قسمت اختصاص الزام مم-کم.۳٫۱ سرویس‌هایی را لیست می‌کند برای آنکه هدف ارزیابی بتواند ارتباطش با موجودیت‌های IT مجاز را راه‌اندازی کند. این الزام نه تنها زمانی به کار می‌رود که ارتباط محافظت شده به صورت اولیه برقرار شده است، بلکه در زمان از سرگیری ارتباط پس از قطع شدن آن نیز کاربرد دارد. ممکن است در مواردی بخشی از تنظمیات هدف ارزیابی شامل تنظیمات دستی راه‌اندازی تونل برای محافظت از ارتباطات دیگر باشد و اگر پس از قطعی، هدف ارزیابی تلاش کند با مداخلات دستی دوباره ارتباط خودکاری راه‌اندازی کند، ممکن است پنجره‌ای ایجاد شود که مهاجم از طریق آن بتواند اطلاعات حساسی را به دست آورد یا اتصال را به خطر اندازد.

شماره	نام خانواده	عنصر امنیتی
الزام		
۷۵	مسیر امن (**FTP_TRP**)	**نام عنصر: مسیر امن ۱** **شماره مؤلفه:** مم-مم.۱۱ (FTP_TRP.1.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید با استفاده از[انتخاب:SSH،IPsec،TLS، TLS/HTTPS]کانال ارتباطی امنی بین خود و سرپرست راه دور ارائه کند که به طور منطقی از دیگر مسیرهای ارتباطی جدا است و به صورت مطمئن نقطه پایانی‌اش را شناسایی می‌کند و از داده‌های مخابره شده در برابر تغییر یا افشاء، محافظت می‌کند.
۷۶		**نام عنصر: مسیر امن ۱** **شماره مؤلفه:** مم-مم.۱۱ (FTP_TRP.1.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید به سرپرستان راه دور اجازه دهند تا ارتباطشان را از طریق مسیر امن راه اندازی کنند.

شماره الزام	نام خانواده
۷۷	عنصر امنیتی

نام عنصر: مسیر امن ۱

شماره مؤلفه: مم-مم.۱۱ (FTP_TRP.1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید ملزم کند که برای احراز هویت اولیه سرپرست و تمام اقدامات سرپرستی راه دور از مسیر امن استفاده کنند.

نکته کاربردی:

این الزام به سرپرست راه دور مجاز این اطمینان را می‌دهد (و دیگر نویسنده‌های هدف امنیتی که نقش آنها مشخص شده است) تمام ارتباطشان با هدف ارزیابی را از طریق مسیر امن راه اندازی کنند و تمام ارتباطات با هدف ارزیابی توسط سرپرستان راه دور بر روی این مسیر انجام گیرد. داده منتقل شده در این کانال ارتباطی امن توسط پروتکل انتخاب شده در این الزام رمز می‌شود. نویسنده هدف امنیتی سازوکار یا سازوکارهای پشتیبانی شده توسط هدف ارزیابی را انتخاب می‌کند. و سپس با توجه به انتخاب انجام شده، الزامات جزئی‌تر متناسب با انتخاب انجام شده از پیوست C در سند هدف امنیتی

شماره	نام خانواده	عنصر امنیتی	الزام
			لحاظ می‌شود.

۸ الزامات تضمین امنیتی

نام کلاس	نام کامپوننت	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests	ATE_IND.1	آزمون مستقل- منطبق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب‌گذاری هدف ارزیابی
	ALC_CMS.1	پوشش پیکربندی هدف ارزیابی

۸,۱ کلاس توسعه

۸,۱,۱ مشخصات کارکردی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱	مشخصات کارکردی	**نام عنصر: مشخصات کارکرد ابتدایی۱**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
	(ADV_FSP)	**شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه دهنده باید مشخصات کارکردی را ارائه کند.
۲		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه کند. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده-سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات هدف ارزیابی» سند هدف امنیتی ارائه شده است، هستند. با توجه به دلایلی که باید در مستندات و بخش «خلاصه مشخصات هدف

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		ارزیابی» وجود داشته باشند، الزامات کارکردی تضمین می‌شوند. از آنجا که مشخصات کارکردی مستقیماً با الزامات کارکرد امنیتی مرتبط شده‌اند، بنابراین ارتباط مطرح شده در این الزام صورت گرفته است و نیازی به مستندات بیشتر نمی‌باشد.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1C)**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی [1] و پشتیبان کننده‌ی الزام کارکرد امنیتی [2] را توصیف کند.
۴		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:** مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص کند.
۵		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.3C)**

[1] SFR-enforcing TSFI

[2] SFR-supporting TSFI

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: مشخصات کارکردی باید برای دسته‌بندی ضمنی واسطهای غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه کند.
۶		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.4C)** **شرح مؤلفه:** ردیابی باید نشان‌دهنده مرتبط شدن الزامات کارکرد امنیتی به واسطهای کارکرد امنیتی در سند مشخصات کارکردی باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۷	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می کند.
۸		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** ارزیاب باید مشخص کند که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی هستند.

۸,۲ کلاس راهنمای کاربر

۸,۲,۱ راهنمای کاربردی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۹	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای کاربردی ارائه کند.

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۰	راهنمای کاربردی **(AGD_OPE)**	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		شرح مؤلفه: سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و مجوزهای دسترسی که باید در یک محیط پردازشی امن کنترل شوند را توصیف کند، همانند هشدارهای مناسب.
۱۱		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.2C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، توصیف کند که چگونه از واسط‌های در دسترس ارائه شده توسط هدف ارزیابی به صورت امن استفاده می‌شود.
۱۲		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.3C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		سند راهنمای کاربردی باید برای هر نقش کاربری، کارکردها و واسطهای دردسترس، به خصوص تمام پارامترهای امنیتی تحت کنترل کاربر را توصیف و مقادیر امن را به صورت مناسبی تعیین کند.
۱۳		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.4C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، هرنوع رویدادهای مربوط به امنیت را به کارکردهای در دسترس کاربر که نیاز است انجام داده شوند، مرتبط کند، همانند تغییر مشخصات امنیتی موجودیت-های تحت کنترل توابع امنیتی هدف ارزیابی.
۱۴		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.5C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		سند راهنمای کاربردی باید تمام مودهای عملیاتی هدف ارزیابی (مودهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و الزامشان برای حفظ عملیات در حالت امن را مشخص کند.
۱۵		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.6C)** **شرح مؤلفه:** سند راهنمای کاربردی باید برای هر نقش کاربری، معیارهای امنیتی که توسط کاربر تبعیت می‌شوند را توصیف کند تا اهداف امنیتی محیط عملیاتی که در سند هدف امنیتی شرح داده شده، کاملاً اجرا شوند.
۱۶		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:** سند راهنمای کاربردی باید واضح و قابل فهم باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۱۷	راهنمای کاربردی (AGD_OPE)	**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده در سند راهنمای کاربردی تمام مؤلفه‌های محتوایی را برآورده می‌کند.

۸,۲,۲ راهنمای آماده‌سازی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
۱۸	راهنمای آماده‌سازی (AGD_PRE)	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		توسعه دهنده باید هدف ارزیابی را همراه با سند آماده‌سازی ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱۹	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** مستندات آماده‌سازی باید تمام مراحل لازم برای پذیرش امن هدف ارزیابی توسط مشتری را مطابق با رویه‌های تحویل توسعه دهنده شرح دهند.
۲۰		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:**

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		مستندات آماده‌سازی باید تمام مراحل لازم برای نصب امن هدف ارزیابی و آماده‌سازی امن محیط عملیاتی را مطابق با اهداف امنیتی محیط عملیاتی ذکر شده در سند هدف امنیتی، شرح دهند.

مؤلفه‌های اقدامات ارزیاب		
۲۱	راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۲۲		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2E)** **شرح مؤلفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید کند، هدف ارزیابی می‌تواند

مؤلفه‌های اقدامات ارزیاب		
		به صورت امن برای عمل کردن آماده شود.

۸,۳ کلاس آزمون

آزمون هدف ارزیابی برای بررسی کارکرد سامانه و جنبه‌هایی که از ضعف طراحی و پیاده‌سازی سود می‌برند، در نظر گرفته می‌شود. آزمون کارکردی سامانه از طریق خانواده ATE_IND و آزمون جنبه‌هایی که از ضعف طراحی و پیاده‌سازی سود می‌برند از طریق خانواده AVA_VAN صورت می‌گیرد. در این سطح از ارزیابی (سطح EAL1) آزمون براساس کارکردی که برای هدف ارزیابی در نظر گرفته شده و واسطهایی که بر اساس اطلاعات طراحی در اختیار قرار می‌گیرند، انجام می‌شود. یکی از خروجی‌های اولیه پروسه ارزیابی گزارش آزمون می‌باشد که در الزامات زیر مشخص شده است.

۸,۳,۱ آزمون مستقل

این دسته از آزمون‌ها برای تائید عملکردی که در بخش «مشخصات امنیتی هدف ارزیابی» و مستندات سرپرستی ارائه شده است، صورت می‌گیرند. تمرکز آزمون‌ها بر روی برآورده شدن الزامات کارکردی مشخص شده در سند هدف امنیتی می‌باشد. فعالیت‌های تضمین حداقل آزمون‌های مربوط به این بخش‌ها را معرفی می کند و ارزیاب گزارشی از طرح آزمون و نتایج آن آماده می کند.

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۳	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
		شماره مؤلفه: (ATE_IND.1.1D) **شرح مؤلفه:** توسعه دهنده باید برای آزمون ، هدف ارزیابی ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۴	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمون باشد.

مؤلفه‌های اقدامات ارزیاب		
۲۵	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، مؤلفه‌های محتوایی را برآورده می‌کند.
۲۶		**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.2E)** **شرح مؤلفه:** ارزیاب باید زیرمجموعه‌ای از توابع امنیتی هدف ارزیابی را آزمون کند تا تائید کند که توابع امنیتی هدف ارزیابی به صورت مشخص شده عمل می‌کنند.

۸,۴ کلاس آسیب‌پذیری

برای آماده نمودن اولیه این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه‌های ارزیابی با تحلیل هدف ارزیابی آن دسته از آسیب‌پذیری‌هایی را که در این نوع محصولات یافت شده‌اند بیابند. غالباً سوء استفاده از این آسیب‌پذیری‌ها(یافتن آسیب‌پذیری‌های در آزمایشگاه) نیاز به مهارت و تخصص مهاجمان دارد.
تا زمانی‌که ابزارهای نفوذ در تمام آزمایشگاه‌ها توزیع می‌شوند و در دسترس هستند، انتظار نمی‌رود که ارزیاب‌ها برای این دسته از آسیب‌پذیری‌های هدف ارزیابی را مورد آزمون قرار دهند. آزمایشگاه‌ها انتظار دارند توضیحاتی پیرامون احتمال کلی این دسته از آسیب‌پذیری‌ها در مستنداتی که توسط فروشنده به کاربران ارائه می‌شود لحاظ شود. اینگونه اطلاعات در توسعه ابزارهای آزمون نفوذ و همچنین نسخه‌های بعدی پروفایل‌های حفاظتی مورد استفاده قرار خواهند گرفت.

۸,۴,۱ تحلیل آسیب‌پذیری

مؤلفه‌های اقدامات توسعه‌دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۷	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه دهنده باید برای آزمون، هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۸	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)** **شرح مؤلفه:** هدف ارزیابی باید مناسب آزمون باشد.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۹	آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده، تمام مؤلفه‌های محتوایی را برآورده می‌کند.
۳۰		**نام عنصر: آسیب‌پذیری ۱**

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
		شماره مؤلفه: (AVA_VAN.1.2E) **شرح مؤلفه:** ارزیاب باید برای شناسایی آسیب‌پذیری‌های بالقوه در هدف ارزیابی، در منابع عمومی جستجویی را انجام دهد.
۳۱		**نام عنصر: آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید براساس آسیب‌پذیری‌های بالقوه شناسایی شده، آزمون نفوذ را انجام دهد تا مقاومت هدف ارزیابی در برابر حملات با توان پایه که توسط مهاجمان صورت می‌گیرند، مشخص کند.

۸,۵ کلاس پشتیبانی از چرخه حیات

در سطح اطمینانی که این پروفایل حفاظتی ارائه شده است (EAL1) کلاس پشتیبانی از چرخه حیات به ویژگی‌هایی از چرخه حیات محدود می‌شود که توسط کاربر نهایی قابل مشاهده باشد. این به معنی نیست که سبک و سیاق توسعه دهنده نقش کمرنگی در قابل اعتماد بودن محصول دارد، بلکه در این سطح اطمینان(EAL1) تنها به این اطلاعات نیاز است.

۸,۵,۱ قابلیت‌های پیکربندی

این مؤلفه جهت معرفی هدف ارزیابی به صورت مجزا از دیگر محصولات یا نسخه‌ای که توسط فروشنده ارائه شده، هست (بدین معنی که جدا ار برچسب‌گذاری محصول، هدف ارزیابی که ممکن است بخشی از یک محصول باشد به تنهایی، برچسب‌گذاری شود، نام هدف ارزیابی، نسخه آن و غیره). بدین ترتیب کاربر نهایی می‌تواند هدف ارزیابی را که توسط مرکز گواهی تائید شده است به آسانی تشخیص دهد.

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۲	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه دهنده باید هدف ارزیابی و مرجع هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۳	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1C)** **شرح مؤلفه:** هدف ارزیابی باید با یک مرجع یکتا برچسب زده شود.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۴	قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب گذاری هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می کند.

۸,۵,۲ حوزه پیکربندی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۵	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** ارزیاب باید لیست پیکربندی هدف ارزیابی را ارائه کند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۶	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید شامل خود هدف ارزیابی و مدارک مورد نیاز توسط الزامات تضمین امنیتی باشد.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۷		**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1C)** **شرح مؤلفه:** لیست پیکربندی باید موارد پیکربندی را به صورت یکتا معرفی کند.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۳۸	حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی هدف ارزیابی ۱** **شماره مؤلفه: (ALC_CMS.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌کند..

۹ پیوست الف

این پیوست شامل عناصر اضافی بدون پشتیبانی از تهدیدها، اهداف، دلایل یا (در برخی موارد) فعالیت‌های تضمین است.

۹,۱ کلاس: ممیزی امنیت

چنانچه بازبینی ممیزی و/یا ذخیره ممیزی توسط هدف ارزیابی پشتیبانی می‌شود، الزامات زیر باید در هدف امنیتی به صورت مناسب در نظر گرفته شود:

شماره	نام خانواده	عنصر امنیتی
الزام		
۳۹	بازبینی ممیزی (FAU_SAR)	**نام عنصر: بازبینی ممیزی ۱** **شماره مؤلفه:** م‌ا-ب‌ز.۱,۱ (FAU_SAR.1.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید سرپرستان مجاز را با قابلیت خواندن تمام داده‌های ممیزی از رکوردهای ممیزی فراهم کند.
۴۰		**نام عنصر: بازبینی ممیزی ۱** **شماره مؤلفه:** م‌ا-ب‌ز.۲,۱ (FAU_SAR.1.2) **شرح مؤلفه:**

شماره	نام خانواده	عنصر امنیتی
الزام		
		توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی را به صورت مناسبی به سرپرستان مجاز ارائه دهد تا اطلاعات را تفسیر کنند.
۴۱		**نام عنصر: بازبینی ممیزی محدود شده ۲** **شماره مؤلفه:** م‌ا-ب‌ز.۱,۲ (FAU_SAR.2.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید مانع تمام کاربران از داشتن دستیابی خواندن به رکوردهای ممیزی در دنباله ممیزی شوند به جز سرپرستان مجاز.
۴۲	بازبینی ممیزی محدود شده (**FAU_STG**)	**نام عنصر: بازبینی ممیزی محدود شده ۱** **شماره مؤلفه:** م‌ا-ذخ.(ت‌س).۱,۴ (FAU_STG_EXT.4.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید سرپرستان مجاز را قادر سازند تا در صورت پر شدن دنباله ممیزی یک یا بیش از یک اقدام زیر را انتخاب کنند:

شماره نام خانواده

الزام

عنصر امنیتی

أ جلوگیری از رویدادهای قابل ممیزی، به جز رویدادهایی که توسط کاربر مجاز صورت گرفته اند.

ب رونویسی رکوردهای ممیزی که قبلاً ذخیره شده‌اند.

نکته کاربردی:

هدف ارزیابی باید سرپرستان مجازی را ارائه دهد تا بتوانند از ممیزی داده‌های از دست رفته توسط جلوگیری نمودن از وقوع رویدادهای قابل ممیزی، جلوگیری کنند. لزومی ندارد اقدامات سرپرستی مجاز تحت این شرایط ممیزی شود. هدف ارزیابی هم‌چنین سرپرستان مجازی ارائه می‌دهد تا رکوردهای ممیزی قدیمی را رونویسی کنند به جای آنکه از رویدادهای قابل ممیزی جلوگیری کنند که ممکن است در برابر حملات منع خدمت محافظت کنند.

۹,۲ کلاس پشتیبانی از رمزنگاری

اگر پروتکلHTTPS به عنوان پروتکل پشتیبانی شده انتخاب شود، این الزام باید در هدف امنیتی در نظر گرفته شود.

شماره الزام	نام خانواده	عنصر امنیتی
۴۳	پروتکل HTTPS (FCS_HTTPS_EXT)	**نام عنصر: پروتکل HTTPS ۱** **شماره مؤلفه:** رز-HTTPS.(ت‌س).۱,۱ (FCS_HTTPS_EXT.1.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید پروتکل HTTPS مطابق با استاندارد RFC 2818 را پیاده‌سازی کند. **نکته کاربردی:**
۴۴		**نام عنصر: پروتکل HTTPS ۱** **شماره مؤلفه:** رز-HTTPS.(ت‌س).۲,۱ (FCS_HTTPS_EXT.1.2) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید با استفاده از TLS مشخص شده در الزام رز-TLS.(ت‌س).۱ پروتکل HTTPS را پیاده‌سازی کند. **نکته کاربردی:**

شماره	نام خانواده	عنصر امنیتی
الزام		
		نویسنده هدف امنیتی باید جزئیات کافی ارائه دهد تا تعیین کند که پیاده‌سازی چگونه مطابق استاندارد معرفی شده است. این امر می‌تواند با اضافه نمودن مؤلفه به این عنصر یا با اضافه نمودن جزئیات به TSS انجام گیرد.
۴۵	پروتکل SSH (FCS_SSH_EXT)	**نام عنصر: پروتکل SSH ۱**
		شماره مؤلفه: رز-SSH.(ت‌س).۱,۱ (FCS_SSH_EXT.1.1)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید پروتکل SSH را مطابق با استاندارد RFC 4251، 4252، 4253 و 4254 پیاده‌سازی کند.
		نکته کاربردی:
		نویسنده هدف امنیتی باید جزئیات کافی ارائه دهد تا چگونگی مطابقت پیاده‌سازی با استانداردهای معرفی شده را تعیین کنند، این امر می‌تواند با اضافه نمودن مؤلفه به این عنصر یا با االضافه نمودن جزئیات به TSS انجام گیرد.

شماره	نام خانواده	عنصر امنیتی
الزام		
۴۶		**نام عنصر: پروتکل SSH ۱**
		شماره مؤلفه: رز-SSH.(ت‌س).۲,۱.۱ (FCS_SSH_EXT.1.2)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید اطمینان دهد که اتصال SSH پس ازآنکه بیش از 2^{28} بسته با استفاده از آن کلید منتقل گردید، کلید مجدداً توزیع می‌شود.
۴۷		**نام عنصر: پروتکل SSH ۱**
		شماره مؤلفه: رز-SSH.(ت‌س).۳,۱.۱ (FCS_SSH_EXT.1.3)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی، باید اطمینان دهند که پروتکل SSH زمان وقفه‌ای را برای احراز هویت تعریف شده در RFC 4252 از [اختصاص: زمان وقفه] پیاده‌سازی می‌کند، و تعداد تلاش احراز هویت منجر به شکست را که کلاینت ممکن است در یک نشست مجزا انجام دهد به [اختصاص: حداکثر تعداد تلاش] محدود کند.

شماره	نام خانواده	عنصر امنیتی
	الزام	

نکته کاربردی:

در اولین اختصاص، نویسنده هدف امنیتی باید یک زمان وقفه از زمان شروع نشست احراز هویت قراردهد تا زمانی‌که احرازهویت ناموفق است، نشت با وقفه مواجه شود.

در دومین اختصاص، حداکثر تعداد تلاش ناموفق جهت احراز هویت مشخص می‌شود، RFC نشان داده است که پس از آنکه به این تعداد تلاش ناموفق صورت گرفت، سرور باید این نشست را از بین ببرد.

۴۸	**نام عنصر: پروتکل SSH ۱**

شماره مؤلفه: رز-SSH.(ت‌س).۴,۱ (FCS_SSH_EXT.1.4)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد که پروتکل SSH پیاده‌سازی شده، سازوکارهای احرازهویت زیر را به صورت توصیف شده در استاندارد RFC 4252: مبتنی بر کلید عمومی، مبتنی بر رمز عبور پشتیبانی می‌کند.

۴۹	**نام عنصر: پروتکل SSH ۱**

شماره	نام خانواده الزام	عنصر امنیتی

شماره مؤلفه: رز-SSH.(ت‌س).۵,۱ (FCS_SSH_EXT.1.5)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد که همان‌طور که در استاندارد RFC 4253 توصیف شده است، بسته‌های بزرگتر از [اختصاص: تعداد بایت] بایت در اتصال انتقال SSH از بین می‌روند.

نکته کاربردی:

RFC 4253 برای پذیرش «بسته‌های بزرگ» در نظرگرفته شده است، با این پیش‌بینی که بسته‌ها باید دارای «اندازه معقول» یا کاهش یافته باشند. باید توسط نویسنده هدف امنیتی قسمت «اختصاص» با حداکثر اندازه بسته‌ی پذیرفته شده، تکمیل شود، بنابراین «اندازه معقول» برای هدف ارزیابی تعریف می‌شود.

۵۰ **نام عنصر: پروتکل SSH ۱**

شماره مؤلفه: رز-SSH.(ت‌س).۶,۱ (FCS_SSH_EXT.1.6)

شرح مؤلفه:

شماره	نام خانواده	عنصر امنیتی
	الزام	

توابع امنیتی هدف ارزیابی باید اطمینان دهد که پیاده‌سازی انتقال SSH از الگوریتم‌های رمزنگاری زیر استفاده می‌کند:

AES-CBC-256-CBC،AES-CBC-128، [اختصاص:

- AEAD_AES_256_GCM
- AEAD_AES_128_GCM:
- هیچ الگوریتم رمزنگاری دیگر].

نکته کاربردی:

در نسخه‌های بعدی این پروفایل حفاظتی، AES-GCM لازم وضروری خواهد بود و CBC اختیاری خواهد بود. در قسمت «اختصاص»، نویسنده هدف امنیتی می‌تواند الگوریتم‌های AES-GCM را انتخاب کند یا اگر AES-GCM پشتیبانی نمی‌شود «هیچ الگوریتم رمزنگاری دیگر» را انتخاب کند. در صورت انتخاب شدن "AES-GCM" باید FCS_COP مربوطه در هدف امنیتی در نظر گرفته شود.

۵۱ **نام عنصر: پروتکل SSH ۱**

شماره مؤلفه: رز-SSH.(تس).۷,۱.۷ (FCS_SSH_EXT.1.7)

شماره	نام خانواده الزام	عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهند که انتقال SSH پیاده‌سازی شده، از SSH_RSA و [انتخاب: PGP-SIGN-RSA،PGP-SIGN-DSS، هیچ الگوریتم کلیدعمومی دیگر] همانند الگوریتم‌های کلید عمومی‌اش استفاده می کند.

نکته کاربردی:

نویسنده هدف امنیتی، الگوریتم کلید عمومی مجاز و لازم را مشخص می‌کند. این الزام سبب می‌شود که SSH-RSA ضرورتاً وجود داشته باشد و می‌تواند ادعای وجود دو الگوریتم دیگر در هدف امنیتی را نیز بکند. نویسنده هدف امنیتی باید انتخاب مناسبی داشته باشد و اگر تنها SSH-RSA پیاده‌سازی شده است، «هیچ الگوریتم کلید عمومی دیگر» را انتخاب می‌کند.

۵۲ **نام عنصر: پروتکل SSH ۱**

شماره مؤلفه: رز-SSH.(ت‌س).۸,۱.۸ (FCS_SSH_EXT.1.8)

شرح مؤلفه:

شماره	نام خانواده	عنصر امنیتی
	الزام	

توابع امنیتی هدف ارزیابی باید اطمینان دهند که الگوریتم تمامیت داده که در اتصال SSH جهت انتقال داده استفاده شده است hmac-sha1 ، [انتخاب: hmac-sha1-96، hmac-md5، hmac-md5-96، بدون هیچ الگوریتم دیگر] است.

نکته کاربردی:

همان‌طور که در RFC مشخص شده است، HMAC-SHA1 نیاز است، اما الگوریتم‌های تمامیت بیشتری وجود دارد که مجاز هستند. نویسنده هدف امنیتی، الگوریتم‌های پیاده‌سازی شده توسط هدف امنیتی را انتخاب می کند. اگر الگوریتم بیشتری وجود نداشته باشد، «بدون هیچ الگوریتم دیگر» انتخاب می‌شود.

۵۳ **نام عنصر: پروتکل SSH ۱**

شماره مؤلفه: رز-SSH.(ت‌س).۹,۱.۱ (FCS_SSH_EXT.1.9)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید اطمینان دهد که تنها سازوکار تبادل کلید مجاز diffie-hellman-group14-sha1 می‌باشد، که برای پروتکل SSH استفاده می‌شود.

۹,۲,۱ پروتکل Transport Layer Security

اگر TLS به عنوان یک پروتکل پشتیبانی انتخاب شود، بنابراین این الزام باید در هدف امنیتی در نظر گرفته شود.

شماره الزام	نام خانواده	عنصر امنیتی
۵۴	پروتکل TLS (FCS_TLS_EXT)	**نام عنصر: پروتکل TLS ۱** **شماره مؤلفه:** رز-TLS.(ت‌س).۱,۱ (FCS_TLS_EXT.1.1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید یک یا بیش از یک پروتکل [انتخاب: TLS 1.0(RFC 2346)، TLS 1.1 (RFC 4346)، TLS 1.2(RFC 5246)] در پشتیبانی از دنباله‌های رمز زیر را، پیاده‌سازی کند: دنباله‌های رمز الزامی: • TLS_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_DHE_RSA_WITH_AES_256_CBC_SHA

شماره	نام خانواده	عنصر امنیتی
الزام		

دنباله‌های رمز اختیاری:

[انتخاب:

هیچکدام

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

].

نکته کاربردی:

نویسنده هدف امنیتی، باید انتخاب و اختصاص مناسبی را داشته باشد تا بتواند TLS پیاده‌سازی شده را منعکس کند. نویسنده هدف امنیتی باید جزئیات کافی ارائه دهد تا بتواند مشخص کند پیاده‌سازی چگونه مطابق استاندارد معرفی شده است. این امر می‌تواند با اضافه نمودن مؤلفه‌هایی به این عنصر، یا با

شماره الزام	نام خانواده عنصر امنیتی
	اضافه نمودن جزئیات بیشتر در TSS صورت گیرد.
	دنباله‌های رمزی که در پیکربندی ارزیابی شده استفاده می‌شوند توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید دنباله‌های رمز اختیاری که پشتیبانی می‌شوند را انتخاب کند؛ در صورتیکه هیچ دنباله رمزی در پشتیبانی از دنباله‌های رمز الزامی وجود نداشته باشد، «هیچکدام» انتخاب می‌شود. الگوریتم‌های دنباله B (RFC 5430) که در بالا لیست شده‌اند، الگوریتم‌های مقدم برای پیاده‌سازی هستند. نسخه‌های بعدی این پروفایل حفاظتی لازم است برای پشتیبانی TLS 1.2 نیاز خواهد بود(RFC 5246). علاوه براین، در نسخه‌های بعدی این پروفایل حفاظتی لازم است که هدف ارزیابی وسیله‌ای پیشنهاد دهد تا تمام تلاش‌های جهت اتصال را با استفاده از نسخه‌های قدیمی پروتکل SSL/TLS انکار کنند.

۹,۳ کلاس حفاظت از توابع امنیتی هدف ارزیابی (FPT)

در برخی موارد هدف ارزیابی، به صورت فیزیکی بین چندین عنصر توزیع می‌شود، ارتباطات بین این عناصر باید محافظت شده باشد.

شماره الزام	نام خانواده	عنصر امنیتی
۵۵	انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی (FPT_ITT)	**نام عنصر: پ انتقال داده‌های داخلی توابع امنیتی هدف ارزیابی به صورت محافظت شده ۱** **شماره مؤلفه:** ح‌ت-اد-۱,۱(۱)((FPT_ITT.1.1(1) **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید زمانی‌که بین بخش‌های مجزای هدف ارزیابی از طریق استفاده از [انتخاب حداقل یکی از: IPsec، SSH، TLS، TLS/HTTPS] انتقال می‌یابند، داده‌شان را از افشاء محافظت کنند و تغییراتش را تشخیص دهند. **نکته کاربردی:** این الزام اطمینان می‌دهد که تمام ارتباطات بین عناصر هدف ارزیابی توسعه یافته، با استفاده از یک کانال ارتباطی رمز شده محافظت می‌شود. داده‌های منتقل شده در این کانال ارتباطی، توسط پروتکلی که در انتخاب اول مشخص شده است، رمز می‌شوند. نویسنده هدف امنیتی سازوکار یا سازوکارهایی را

شماره	نام خانواده	عنصر امنیتی
الزام		
		انتخاب می کند که توسط هدف ارزیابی پشتیبانی شود و این اطمینان را می‌دهد که جزئیات الزام در این پیوست، مربوط به انتخابی که کرده‌اند (توسط نویسنده هدف امنیتی) در صورتی‌که در سند هدف امنیتی وجود نداشته باشد، کپی می‌شوند.

۹,۴ الزامات ممیزی

با توجه به الزامات خاصی که توسط نویسنده هدف امنیتی از این پیوست انتخاب شده است، نویسنده هدف امنیتی باید رویدادهای قابل ممیزی مناسبی را در هدف امنیتی برای الزام انتخاب شده درنظر بگیرد.

الزامات	رویدادهای قابل ممیزی	محتویات رکوردهای قابل ممیزی بیشتر
رز-TLS.(ت‌س).۱	شکست پروتکل	دلیل شکست
	برقراری/پایان نشست TLS	نقطه پایانی غیرهدف ارزیابی اتصال (آدرس IP) برای شکست و موفقیت
رز-SSL.(ت‌س).۱	شکست پروتکل	دلیل شکست

	برقراری/پایان نشست SSL	نقطه پایانی غیرهدف ارزیابی اتصال (آدرس IP) برای شکست و موفقیت
رز-HTTPS.(ت‌س).۱	شکست پروتکل	دلیل شکست
	برقراری/پایان نشست HTTPS	نقطه پایانی غیرهدف ارزیابی اتصال (آدرس IP) برای شکست و موفقیت
ح‌ت-اد.۱	هیچکدام	