به نام خدا

پروفایل حفاظتی کلاینت بی‌سیم

نسخه ۱,۵

مرداد ۹۳

پیش‌گفتار

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

در بخش اول، Wireless Client به صورت کلی معرفی شده است. سپس در بخشی تحت عنوان «مسائل امنیتی» تهدیداتی که محصول با آنها روبرو است و فرضیاتی که در رابطه با امنیت محصول در نظر گرفته شده است و همچنین خط‌مشی‌های آن عنوان می‌شوند.

سپس در بخش «اهداف امنیتی» مواردی جهت مقابله با تهدیدات، 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 که هریک از این کلاس‌ها حوزه‌ی خاصی از امنیت را پوشش می‌دهند. کلاس‌هایی که برای کلاینت بی‌سیم در این سند مطرح شده، 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 کانال‌ها و مسیرهای مورد اعتماد

هریک از این کلاس‌ها، از مجموعه‌ای از خانواده‌ها تشکیل یافته و هر خانواده از مجموعه‌ای مؤلفه و هر مؤلفه از مجموعه‌ای از عناصر تشکیل یافته است. با استفاده از «الزامات کارکرد امنیتی» در واقع «اهداف امنیتی» بر مبنای استاندارد معیارمشترک بیان می‌شود.

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

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 کردن الزامات ارائه شده‌اند در محصول خود فراهم کنند و به خریداران آن محصول نیز در انتخاب محصول خود کمک کنند. مرکز گواهی امنیتی این سند را در راستای این هدف تهیه کند است.

۲ معرفی اصطلاحات

- **هدف ارزیابی (TOE)**

به سیستم 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])**

1 Non-Target Of Evaluation

2 Protection Profile

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

- **هدف امنیتی (ST[1])**

بیانیه‌ای از 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 می‌کند.

این بیانیه شامل موارد زیر است:

- «تهدیداتی» 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])**

1 Security Target

2 Organizational Security Policy

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.

- **اهداف امنیتی (Security Objective)**

در سندهای «هدف امنیتی» و «پروفایل حفاظتی» بخشی تحت عنوان «اهداف امنیتی» وجود دارد که برای مقابله با تهدیدات معرفی شده و/یا برای برآورده نمودن 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 می‌شود تا در حاصل شدن اهداف ارزیابی، برای هدف ارزیابی کمک کنند.

- **الزام کارکرد امنیتی(SFR[1])**

بیان کننده‌ی 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.

1 Security Functional Requirement

2 Security Assurance Requirement

- **بسته (Package)**

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

- **سطح تضمین ارزیابی(EAL[1])**

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

- **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)**

1 Evaluation Assurance Level

2 TOE Security Functions

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 است.

- **کلاس (Class)**

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

- **انتخاب (Selection)**

---

۱ در استاندارد ملی ISO 15408 منتشر شده توسط سازمان ملی استاندارد ایران، Component مؤلفه ترجمه شده است.

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

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

- **سرپرست (Administrator)**

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 سیستم 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 سیستم مورد ارزیابی (هدف ارزیابی) می‌باشد که شامل اطلاعات است و یا اطلاعات را دریافت می‌کند 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 می‌شود 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 نمایند.

- **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 شده 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 مؤلفه‌های کارکرد امنیتی بوده که مبنایی برای ارزیابی الزامات کارکرد امنیتی موجود در پروفایل حفاظتی یا سند هدف امنیتی است. این الزامات به توضیح رفتارهای امنیتی مورد نظر هدف ارزیابی[2] یا محیط فناوری اطلاعات پرداخته و هدف آن برآورده کردن اهداف امنیتی است که در پروفایل حفاظتی یا سند هدف امنیتی تعیین شده‌اند.

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

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

بخش دوم: الزامات کارکرد امنیتی [3]

بخش سوم: الزامات تضمین امنیتی[1]

---

1 Common Criteria (CC)

2 Target Of Evaluation (TOE)

3 Security Functional Requirement (SFR)

۴ معرفی تجهیزات کلاینت بی‌سیم

این سند الزامات کارکرد امنیتی برای کلاینت WLAN را مشخص کرده است. هدف ارزیابی که در این پروفایل حفاظتی تعریف شده است، عنصری است که بر روی ماشین کلاینت اجرا می‌شود(اغلب به یک «کلاینت دسترسی از راه دور» اشاره دارد).

هدف ارزیابی یک تونل بی‌سیم امن بین تجهیزات کلاینت و سیستم دسترسی از راه دور برقرار می‌کند که از طریق آن تمام داده‌ها پیمایش خواهند شد. سیستم دسترسی از راه دور اطمینان می‌دهد که تنها کلاینت‌های مجاز از طریق احراز هویت شدن با یک سرور احراز هویت، این دسترسی را به دست خواهند آورد. این پروفایل حفاظتی هیچ پیکربندی خاصی را تحمیل نمی‌کند. در عوض این پروفایل حفاظتی الزامات امنیتی را برای کلاینت فراهم می‌آورد که ارتباط بین کاربر بی‌سیم و شبکه با سیم[۲] فراهم می‌کند. همان‌طور که در بخش زیر بحث شده است، مهم آن است تاکید شود که پروفایل حفاظتی تنها عملکرد کلاینت WLAN و قابلیت‌های سرپرستی را پوشش می‌دهد و تحمیل کننده‌ی الزاماتی همانند شناسایی و احراز هویت و ذخیره ممیزی و غیره که در محیط IT پیاده‌سازی خواهند شد، نیست. این قابلیت‌ها باید مطابق با الزامات مشخص شده برای سیستم‌عامل باشد؛ برای مثال:

کلاینت WLAN از استاندارد IEEE 802.1X کنترل دسترسی شبکه مبتنی بر پورت را پشتیبانی می‌کند. چارچوب معماری کنترل دسترسی مبتنی بر پورت، سه نقش مجزا را تعریف می‌کند:

- درخواست کننده (هدف ارزیابی)

---

1 Security Assurance Requirement (SAR)

2 Wired network

- تائید کننده اعتبار (سیستم دسترسی WLAN)
- سرور احراز هویت‌کننده (AS)

سیستم دسترسی WLAN نیاز به احراز هویت موفق هدف ارزیابی با تکیه بر AS دارد، پیش از آنکه دسترسی به شبکه فراهم شود. اقدامات سیستم دسترسی WLAN از طریق تجهیزات بین هدف ارزیابی و AS رخ می‌دهد. سیستم دسترسی WLAN به کلاینت WLAN اجازه می‌دهد تا به شبکه خصوصی تنها بعد از احراز هویت موفق توسط AS دسترسی داشته باشد. هدف ارزیابی و AS باید به صورت متقابل با استفاده ازگواهینامه‌های X.509 v3 و پیغام‌های EAP-TLS[1] احراز هویت متقابل انجام دهند. اگر احراز هویت AS یا هدف ارزیابی با شکست مواجه شود، سیستم دسترسی WLAN ارتباطش را با کلاینت WLAN قطع می‌کند.

تونل‌های ارتباطی امن به شبکه خصوصی تنها زمانی می‌تواند برقرار شود که احراز هویت با موفقیت انجام شود.

۴,۱ استفاده و ویژگی‌های امنیتی اصلی هدف ارزیابی

کلاینت WLAN به کاربران راه دور اجازه می‌دهد تا از ماشین کلاینت جهت برقراری ارتباط بدون سیم با شبکه خصوصی استفاده کند. بسته‌های IP، که بین شبکه خصوصی و یک کلاینت WLAN دسترسی از راه دور در حال انتقال است، به صورت رمز شده هستند. کلاینت WLAN از داده بین خودش و شبکه خصوصی محافظت می‌کند و محرمانگی و یکپارچگی و صحت را ارائه می‌دهد و از داده در حال انتقال محافظت می‌کند حتی اگر این کلاینت یک اتصال بی سیم را پیمایش کند.

الزامات عملکرد امنیتی اصلی در این پروفایل حفاظتی جنبه‌های اساسی زیر از کلاینت WLAN هستند:

1 Extensible Authentication Protocol – Transport Layer Security

- احراز هویت کلاینت WLAN
- احراز هویت سرور احراز هویت
- محافظت رمزنگاری از داده‌ای که منتقل می‌شود
- پیاده‌سازی سرویس‌ها

کلاینت WLAN یک تونل 802.11 بین تجهیزات کلاینت و زیر ساخت شبکه با استفاده از IEEE 802.1X با EAP-TLS برای احراز هویت برقرار می‌کند. این کلاینت یک احراز هویت متقابل با AS در شبکه خصوصی به عنوان بخشی از تبادلات EAP-TLS انجام می‌دهد. تبادلات EAP-TLS از گواهینامه‌های ماشین برای احراز هویت متقابل استفاده می‌کند. کلاینت WLAN گواهی‌نامه ماشین منتقل شده از AS و اعتبار سنجی آن را بررسی می‌کند و اطمینان می‌دهد که گواهی‌نامه توسط سازمان صدور گواهی-نامه [1]به صورت امن امضاء شده است. AS هم‌زمان گواهی‌نامه کلاینت WLAN را احراز هویت می‌کند. زمانی‌که تبادلات EAP-TLS با موفقیت تکمیل شد، شبکه به کلاینت WLAN اجازه می‌دهد که به برقراری یک تونل ارتباطی امن با شبکه خصوصی پایان بدهد. کلاینت WLAN یک کانال رمز شده و احراز هویت شده را با سیستم دسترسی WLAN با استفاده از دست‌داد چهار طرفه[2] که در استاندارد IEEE 802.11 مشخص شده است، برقرار کند. هنگامی‌که چنین کانالی برقرار شد، تمام ارتباطات بین کلاینت WLAN به سیستم دسترسی WLAN با AES در مد CCMP (به صورت مشخص شده در استاندارد IEEE 802.11) رمز می‌شود.

1 Certificate Authority(CA)

2 4way handshake

کلاینت WLAN که در این پروفایل حفاظتی تعریف شده است، یک عنصر اجرایی بر روی ماشین کلاینت دسترسی از راه دور است. توجه شود که کلاینت نشان داده شده تنها بخش کوچکی از «ماشین» کلاینت WLAN می‌باشد. بدین ترتیب، هدف ارزیابی باید به شدت به محیط عملیاتی هدف ارزیابی (پلتفرم میزبان، پشته شبکه و سامانه عامل) جهت دامنه اجراییش و استفاده مناسب تکیه کند. هدف ارزیابی به محیط IT تکیه می‌کند تا بخشی از عملکرد امنیتی مربوط به کارکرد سرپرست را نشان دهد. فرض بر این است که کلاینت WLAN به درستی پیاده‌سازی شود و هیچ اشتباه طراحی مهمی نداشته باشد. ویژگی‌های امنیتی هدف ارزیابی، شامل سرپرستی، تطبیق پروتکل، حفاظت رمزنگاری و تولید ممیزی است. کلاینت WLAN برای اجرا شدن صحیح و ساز و کارهای حفاظتی ماشین کلاینت زیر به محیط IT متکی است:

- بازبینی ممیزی
- ذخیره ممیزی
- شناسایی و احراز هویت
- مدیریت امنیتی
- مدیریت نشست

لازم است فروشنده راهنمای پیکربندی ارائه دهد (AGD_PRE، AGD_OPE) تا ماشین کلاینت و هدف ارزیابی را برای هر محیط عملیاتی پشتیبانی شده به طور صحیح نصب و پیکربندی کند.

۴,۲ رمزنگاری

کلاینت WLAN به عملکرد رمزنگاری جهت ارائه دادن محرمانگی، صحت و یکپارچگی و حفاظت از داده منتقل شده متکی است. انتظار می‌رود کلاینت WLAN جریان ترافیک بی‌سیم بین دو تجهیز را که از نظر جغرافیایی مجزا هستند رمز کند. کلاینتWLAN به عنوان یک نقطه انتهایی برای تونل WLAN به کار می‌رود و برخی از عملکردهای رمزنگاری مربوط به برقراری و نگهداری تونل را انجام می‌دهد. با استفاده از پروتکل‌ها و الگوریتم‌های استاندارد، کلاینت WLAN اطمینان می‌دهد که هر پیغام امن است حتی زمانی‌که در شبکه بی‌سیم پیمایش می‌کند. الگوریتم رمزنگاری AES در مد CCMP جهت حفاظت از داده‌های منتقل شده استفاده می‌شود. مد CCMP بر اساس دو مد بلاک رمزنگاری در حالت ترکیبی است (مد شمارنده که محرمانگی را ارائه می‌دهد و بلاک رمزنگاری متوالی کد احراز اصالت پیغام (CBC-MAC) که صحت داده را ارائه می‌دهد).

چنان‌چه از رمزنگاری جهت احراز هویت، تولید کلید و رمزنگاری اطلاعات که به اندازه کافی ایمن هستند استفاده شود و پیاده‌سازی شامل اشتباهات طراحی حساسی نباشد، مهاجم قادر به جستجوی فراگیر فضای کلید رمزنگاری جهت به دست آوردن داده‌های بی سیم نخواهد بود. فن‌آوری WPA2[1] همان‌گونه که در استانداردهای IEEE802.11 و IEEE802.1X مشخص شده است، RBG و عوامل احراز هویت امن تضمین خواهند کرد که دستیابی به اطلاعات منتقل شده نمی‌تواند با کاری کمتر از جستجوی فراگیر کامل فضای کلید به دست آید. هر متن اصلی راز و کلید خصوصی یا دیگر پارامترهای امنیتی رمزنگاری زمانی که دیگر استفاده نمی‌شوند صفر خواهند شد تا از افشای داده‌های حساس امنیتی جلوگیری کنند.

1 Wireless Protected Access 2

۵ مسائل امنیتی

۵,۱ تهدیدات

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.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 یک 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 داده‌های 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.

۵,۲ خط مشی‌ها

P.TYPE	توضیحات
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.CONFIGURABILITY	هدف ارزیابی باید قادر به تنظیم و پیکربندی جنبه‌های امنیتی عملکردش باشد.

۵,۳ فرضیات

P.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.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.

۵,۴ اهداف امنیتی

۵,۴,۱ 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 نمود تا اطمینان نمود که بروزرسانی هدف ارزیابی توسط سرپرست تائید شده، بدون تغییر و از یک منبع قابل اطمینان می‌باشد.
O.SYSTEM_MONITORING	هدف ارزیابی قابلیتی برای تولید داده‌های ممیزی و فرستادن این داده‌ها به یک موجودیت IT خارجی فراهم خواهد نمود.
O.CRYPTOGRAPHIC_FUNCTIONS	هدف ارزیابی باید عملکرد رمزنگاری داشته باشد تا بتواند محرمانگی را حفظ کند و امکان تشخیص تغییرات داده‌ای را که به خارج از هدف ارزیابی و محیط میزبان منتقل می‌شود فراهم کند.
O.TOE_ADMINISTRATION	هدف ارزیابی سازوکارهایی ارائه خواهد داد تا سرپرستان قادر به پیکربندی هدف ارزیابی باشند.
O.RESIDUAL_INFORMATION_CLEARING	هدف ارزیابی اطمینان خواهد داد هیچ یک از داده‌های یک منبع محافظت شده در زمان تخصیص مجدد منبع، در دسترس قرار نخواهند گرفت.
O.WIRELESS_ACCESS_POINT_CONNECTION	هدف ارزیابی باید قادر به محدود نمودن نقاط دسترسی بی‌سیمی که به آن متصل خواهند شد، باشد.
O.TSF_SELF_TEST	هدف ارزیابی قابلیتی جهت آزمودن برخی از زیر مجموعه عملکردهای امنیتی خود ارائه خواهد کرد تا از عملکرد مناسب آنها اطمینان حاصل کند.

۵,۴,۲ اهداف امنیتی محیط عملیاتی

OE.TYPE	توضیحات
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 کردن و به کاربردن مطمئن تمام راهنماهای سرپرستی، قابل اعتماد می‌باشند.

۶ الزامات کارکرد امنیتی کلاینت 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.

۶,۱ کلاس ممیزی امنیت

نام کلاس: ممیزی امنیت

شرح کلاس: Wireless Client ها 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 کرده 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 سیستم در برخورد با خطاهای امنیتی[1]**

این خانواده تعریف کننده الزامات برای واکنش‌های سیستم 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 را که باید توسط توابع امنیتی هدف ارزیابی قابل ممیزی باشند 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 سیستم 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[4]**

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

---

1 Security audit automatic response (FAU_ARP)

2 Security audit data generation (FAU_GEN)

3 Security audit analysis (FAU_SAA)

4 Security audit review (FAU_SAR)

- **خانواده انتخاب رویدادهای ممیزی امنیت[1]**

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

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

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:** توابع امنیتی هدف ارزیابی باید بتوانند از رویدادهای قابل ممیزی زیر یک رکورد ممیزی تولید کنند : الف- آغاز و پایان توابع ممیزی

1 Security audit event selection (FAU_SEL)

2 Security audit event storage (FAU_STG)

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-اخ.۱ **FAU_SEL.1**	تمامی تغییرات پیکربندی ممیزی هنگامی رخ می‌دهد که عمل جمع‌آوری ممیزی انجام می‌گیرد.	هیچ
رز-م‌ک.۱ **FCS_CKM.1**	شکست فعالیت تولید کلید	هیچ
رز-م‌ک.۲ **FCS_CKM.2**	شکست فعالیت توزیع کلید	هیچ
رز-م‌ک.(ت‌س).۴ **FCS_CKM_EXT.4**	شکست فرآیند صفرسازی کلید	هویت موجودیت فعال یا موجودیت حذف شده
رز-ع‌ر.۱(۱) **FCS_COP.1(1)**	شکست رمزنگاری یا رمزگشایی	مد عملیات رمزنگاری ، نام/شناسه موجودیت غیرفعال رمز شده/رمزگشایی شده
رز-ع‌ر.۱(۲) **FCS_COP.1(2)**	شکست امضاء رمزنگاری	مد رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال رمز شده/بررسی شده

رز-ع‌ر.۱(۳) **FCS_COP.1(3)**	شکست تابع درهم‌سازی	مد رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال درهم‌سازی شده
رز-ع‌ر.۱(۴) **FCS_COP.1(4)**	شکست در درهم‌سازی رمزنگاری برای یکپارچگی غیرداده[1]	مد رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال درهم‌سازی شده
رز-ع‌ر.۱(۵) **FCS_COP.1(5)**	شکست رمزنگاری یا رمزگشایی WPA2	مد رمزنگاری عملیات، نام/شناسه موجودیت غیرفعال رمز شده/رمزگشایی شده، غیر هدف ارزیابی بودن نقطه پایانی اتصال (آدرس IP)
رز-پا-ل‌ا.(ت‌س).۱ **FCS_EAP_TLS_EXT.1**	شکست پروتکل شکست احراز هویت	دلیل شکست نقطه پایانی اتصال غیر هدف ارزیابی (آدرس IP) برای موفقیت و شکست
اش-مع.(ت‌س).۱ **FIA_RBG_EXT.1**	شکست فرآیند تصادفی‌سازی	هیچ
اش-ش‌ه.(ت‌س).۱ **FDP_RIP.2**	هیچ	
اش-8021X.(ت‌س).۱ **FIA_8021X_EXT.1**	تلاش جهت دستیابی به پورت کنترل شده 802.1X	هویت کلاینت ارائه شده (آدرس IP)
اش-509 X .(ت‌س).۱ **FIA_X509_EXT.1**	هیچ	

1 Non-Data

ح‌ت-خا.(ت‌س).۱ **FPT_TST_EXT.1**	اجـرای مجموعـه آزمـون‌هـای خودآزمایی توابع امنیتـی هـدف ارزیابی. نقض‌های یکپارچگی تشـخیص-داده شده	برای نقض یکپارچگی، فایل کد توابع امنیتـی هـدف ارزیابی که سبب نقض یکپارچگی می‌شود.
ح‌ت-رم.(ت‌س).۱ **FPT_TUD_EXT.1**	شروع به روزرسانی. هرگونـه شکسـت در بررسـی یکپارچگی به‌روزرسانی.	بدون هیچ اطلاعات اضافه
مد-ع‌م.۱ **FMT_SMF.1**	هیچ	
دس-ب‌ن.(ت‌س).۱ **FTA_WSE_EXT.1**	تمام تلاش برای اتصال به نقطه دسترسی	هویت نقطه دسترسی که متصل می‌شود.
مم-ک‌م.۱ **FTP_ITC.1**	تمام تلاش برای برقراری یک کانال امن. تشخیص تغییرات داده‌ی موجود در کانال.	شناسایی نقطه انتهایی غیر هدف ازریابی کانل

نکته کاربردی:

نویسنده هدف امنیتی می‌تواند رویدادهای ممیزی دیگری را در این جدول لحاظ کند. بدین معنا که رویدادها محدود بـه جـدول فـوق

نیستند.

در بند «الف»، عملیات ممیزی به آن دسته عملیاتی اشاره دارد که توسط هدف ارزیابی ارائه شده است. برای مثال، درمواردی که هدف ارزیابی به تنهایی قابل اجرا است، آغاز و پایان عملیات ممیزی هدف ارزیابی جهت برآوردن الزامات این بند کافی خواهد بود.

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 باشند، بنابراین هیچ ویژگی اضافی از این فعالیت‌های قابل ممیزی در جدول ۱ مشخص نشده است.

هدف ارزیابی نیازی به ارائه دادن قابلیتی جهت شناسایی و احراز هویت سرپرست ندارد، این الزام حاکی از آن است که هدف ارزیابی قادر به ممیزی رویدادهای توصیف شده توسط پروفایل حفاظتی به صورت «اقدامات سرپرستی» است. انتظار می‌رود که راهنمای OPE مراحل ضروری را با جزییات نشان دهد تا اطمینان دهد که داده ممیزی تولید شده توسط هدف ارزیابی با قابلیت‌های ممیزی اصولی IT یکپارچه شود.

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

شماره مؤلفه: ما-ت‌ل.۲,۱.۱(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: 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 بر اساس دارا بودن/ نبودن ویژگی‌های زیر از مجموعه رویدادهای ممیزی را داشته باشد :

الف- نوع رویداد

موفقیت رویداد امنیتی قابل ممیزی

شکست رویداد امنیتی قابل ممیزی

ب- [اختصاص: دیگر ویژگی‌ها].

نکته کاربردی:

منظور این الزام آن است که تمام معیارهایی را که می‌تواند 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.

۶,۲ 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 می‌تواند شامل موارد زیر باشد اما تنها به این دسته نیز محدود نمی‌شود:

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

این کلاس زمانی که هدف ارزیابی، عملکرد رمزنگاری را پیاده‌سازی می‌کند، استفاده می‌شود این پیاده‌سازی در نرم‌افزار، سخت‌افزار و میان افزار می‌تواند صورت گیرد.

➢ خانواده مدیریت کلید رمزنگاری

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

- 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

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 امضاء دیجیتال، تولید کنترل [۱]رمزنگاری برای یکپارچگی و یا تائید کنترل، درهم‌سازی امن (خلاصه پیام)، رمزنگاری و/یا رمزگشایی کلید رمزنگاری، و توافق کلید رمزنگاری می‌باشد.

[۱] checksum

شماره الزام	نام خانواده	عنصر امنیتی
۴	تولید کلید رمزنگاری (FCS_CKM)	**نام عنصر: مدیریت کلید رمزنگاری ۱** **شماره مؤلفه: رز-م‌ک.۱,۱ (FCS_CKM.1.1)** **شرح مؤلفه :** توابع امنیتی هدف ارزیابی باید کلیدهای رمزنگاری متقارن را 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] برآورده می‌کند، استخراج کند. **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.
۵		**نام عنصر: توزیع کلید رمزنگاری(GTK) ۲** **شماره مؤلفه: رز-م‌ک.۱,۲ (FCS_CKM.2.1)**

شماره الزام	نام خانواده	عنصر امنیتی

شرح مؤلفه :

توابع امنیتی هدف ارزیابی باید کلید موقتی گروهی[1] را مطابق با یک روش توزیع کلید رمزنگاری خاص: [کلید AES پنهان شده در یک قالب کلید EAPOL] که استاندارد: [RFC 3394 برای پنهان کردن کلید رمزنگاری، 802.11-2007 برای فرمت بسته‌ها و در نظر گرفتن زمان] را برآورده کند و کلیدهای رمزنگاری افشاء نمی‌نمایند، توزیع کند.

نکته کاربردی:

این الزام به کلید موقتی گروهی (GTK) اعمال می‌شود این کلید توسط هدف ارزیابی دریافت شده و برای رمزگشایی پیغام‌های پخشی و چند پخشی از نقطه دسترسی به آنچه که متصل شده است، استفاده می‌شود. استاندارد 802.11-2007 فرمتی را برای انتقال مشخص می-کند درواقع باید توسط روش پنهان‌سازی کلید AES که در RFC 3394 مشخص شده است، پنهان شود؛ هدف ارزیابی باید قادر به آشکارسازی چنین کلیدهایی باشد.

۶	**نام عنصر: صفرسازی کلید رمزنگاری ۴** **شماره مؤلفه: رز-م‌ک-(ت‌س).۱,۴ (FCS_CKM.4.1)**

1 Group Temporal Key

شماره **نام خانواده**

الزام

عنصر امنیتی

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.

عمل صفرسازی کلید که در این الزام به آن اشاره شده است، به محض آنکه از کلید/CSP به موقعیت دیگر منتقل می‌شود به هر فضای ذخیره‌سازی میانی (یعنی هر دستگاه ذخیره‌سازی مانند بافرهای حافظه که در مسیر چنین داده‌هایی قرارداده شده‌اند)برای کلیدهای مخفی و پارامترهای امنیتی رمزنگاری (CSP) اعمال می‌شود.

چون هدف ارزیابی لزوماً دربرگیرنده‌ی محیط فناوری اطلاعات میزبان نمی‌شود، مقدار این قابلیت تا اندازه‌ای محدود شده است. به منظور برآورده کردن این الزام ، کافی است هدف ارزیابی عملکرد اصولی درست میزبان را برای انجام عمل صفرسازی، فراخوانی کند. این کار بر این دلالات ندارد که هدف ارزیابی باید شامل راه انداز حافظه در مود کرنل باشد تا از صفرشدن داده ها اطمینان حاصل شود.

شماره الزام	نام خانواده	عنصر امنیتی
۷		**نام عنصر: عملیات رمزنگاری(برای رمزنگاری/رمزگشایی داده) ۱ (۱)**
		شماره مؤلفه: رز-ع‌ر.۱,۱ (۱)((FCS_COP.1.1(1))
		شرح مؤلفه:
	عملیات رمزنگاری (**FCS_COP**)	توابع امنیتی هدف ارزیابی باید [کدبندی و کدگشایی] را مطابق با الگوریتم رمزنگاری مشخص شده [AES که در[اختصاص: یک یا بیش از یک مد]] عمل می‌کند و اندازه‌های کلید رمزنگاری ۱۲۸ و ۲۵۶ بیتی و [انتخاب : ۱۹۲ بیتی ، نه هیچ اندازه دیگری]را 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 800-38E]
		نکته کاربردی:
		در قسمت «اختصاص»، نویسنده هدف امنیتی باید مد یا مدهایی را که در آن مدها AES عمل می‌کند 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 امنیتی باید استانداردهایی راانتخاب کند که مدهای مشخص شده در قسمت «اختصاص» را توصیف می‌کند. قابل ذکر است که این الزام به رمزنگاری ترافیک بی‌سیم اعمال نمی‌شود. الزام رز-ع‌ر.۱(۵) مد، اندازه کلید و استانداردهایی را تعریف می-

شماره	نام خانواده	عنصر امنیتی
الزام		

کند که برای رمزنگاری/رمزگشایی WPA2 بدون سیم استفاده می‌شود.

۸ **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 :

۱- الگوریتم امضای دیجیتال (DSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با FIPS PUB 186-3، «استاندارد امضای دیجیتال»
۲- الگوریتم امضای دیجیتال RSA (rDSA) با کلید ۲۰۴۸ بیتی یا بیشتر مطابق با FIPS PUB 186-3، «استاندارد امضای دیجیتال»
۳- الگوریتم امضای دیجیتال منحنی بیضوی (ECDSA[1]) با کلید ۲۵۶ بیتی یا بیشتر مطابق با

a. [انتخاب: FIPS PUB 186-3، «استاندارد امضای دیجیتال»]
b. تابع ارزیابی امنیتی باید «منحنی‌های استاندارد « NIST curve»، P-256، P384 و [انتخاب : P251 ، نه سایر منحنی‌ها] (هم‌چنان‌که در FIPS PUB 186-3، «استاندارد امضای دیجیتال» تعریف شده‌است)] را پیاده‌سازی کند..

نکته کاربردی:

نویسنده هدف امنیتی باید الگوریتم پیاده‌سازی شده را برای امضاء دیجیتال انتخاب کند؛ اگر بیش از یک الگوریتم در دسترس باشد، این

1 Elliptic Curve Digital Signature Algorithm

شماره الزام	نام خانواده عنصر امنیتی
	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.
۹	**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 خلاصه پیام قابل قبول ۱۶۰ بیت خواهد بود.

1 Message Digest Sizes

شماره	نام خانواده	عنصر امنیتی
الزام		
۱۰		**نام عنصر: عملیات رمزنگاری ۱(۴)**

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

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید [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-سازی یک گام مناسب در طیفی از برنامه‌های کاربردی است. کوتاه شدن پیام، اندازه خروجی نهایی و استانداردی که پیام کوتاه شده

شماره الزام	نام خانواده	عنصر امنیتی
		منطبق برآن است باید در هدف امنیتی بیان شود.
۱۱		**نام عنصر: عملیات رمزنگاری(رمزنگاری و 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 مشخصAES 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 با انطباق به استاندارد IEEE 802.11-2007، AES CCMP با اندازه کلید رمزنگاری ۱۲۸ بیت باید پیاده‌سازی شود. در آینده این استاندارد به روزرسانی خواهد شد و مدهای رمزنگاری جدید بازبینی می‌شود و توسط NIST تصویب می‌شود، این الزام ممکن است شامل الزاماتی برای مدهای رمزنگاری جدید/اضافی و اندازه کلید باشد.
۱۲	پروتکل EAP-TLS (	**نام عنصر: پروتکل EAP-TLS ۱**
		شماره مؤلفه: رز-پ‌ا-ل‌ا-(ت‌س).۱،۱ (FCS_IPSEC_EXT.1.1)

شماره الزام	نام خانواده	عنصر امنیتی
FCS_EAP_TLS_EXT)	شرح مؤلفه:	

توابع امنیتی هدف ارزیابی باید پروتکل EAP-TLS به صورت مشخص شده در RFC 5216 پیاده‌سازی کند تا از دنباله رمزهای زیر پشتیبانی کند:

- دنباله رمز الزامی مطابق با RFC 3268:

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

- دنباله رمز اختیاری:

[انتخاب:

هیچکدام

TLS_RSA_WITH_AES_128_CBC_SHA 256به صورت تعریف شده در RFC 5246

TLS_RSA_WITH_AES_256_CBC_SHA256به صورت تعریف شده در RFC 5246

شماره	نام خانواده	عنصر امنیتی	الزام
		TLS_DHE_RSA_WITH_AES_128_CBC_SHA256به صورت تعریف شده در RFC 5246	
		TLS_DHE_RSA_WITH_AES_256_CBC_SHA256به صورت تعریف شده در RFC 5246	
		TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256به صورت تعریف شده در RFC 5289	
		TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384به صورت تعریف شده در RFC 5289	
		TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256به صورت تعریف شده در RFC 5430	
		TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384به صورت تعریف شده در RFC 5430	

].

۱۳ **نام عنصر: پروتکل EAP-TLS ۱**

شماره مؤلفه: رز-پا-ل‌ا-(ت‌س).۲,۱.۱ (FCS_IPSEC_EXT.1.2)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید با استفاده از RBG مشخص شده در رز-ب‌ت.(ت‌س).۱ مقادیر تصادفی تولید کند که در تبادلات EAP-TLS استفاده می‌شود.

شماره الزام	نام خانواده	عنصر امنیتی
۱۴		**نام عنصر: پروتکل EAP-TLS ۱** **شماره مؤلفه: رز-پا-ل‌ا-(ت‌س).۳,۱ (FCS_IPSEC_EXT.1.3)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از گواهینامه X509 v3 به صورت مشخص شده در اش-X509.(ت‌س).۱ استفاده کند.
۱۵		**نام عنصر: پروتکل EAP-TLS ۱** **شماره مؤلفه: رز-پا-ل‌ا-(ت‌س).۴,۱ (FCS_IPSEC_EXT.1.4)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تائید کند که گواهینامه سرور ارائه شده، شامل احراز هویت سرور در نظر گرفته شده در فیلد KeyUsage توسعه یافته است.
۱۶		**نام عنصر: پروتکل EAP-TLS ۱** **شماره مؤلفه: رز-پا-ل‌ا-(ت‌س).۴,۱ (FCS_IPSEC_EXT.1.4)** **شرح مؤلفه:**

شماره	نام خانواده	عنصر امنیتی
الزام		
		توابع امنیتی هدف ارزیابی باید به سرپرست مجاز اجازه بدهند تا لیست CA هایی را که مجاز به امضاء گواهی‌نامه‌های سرور احراز هویت پذیرفته شده توسط هدف ارزیابی هستند پیکربندی کند.
۱۷		**نام عنصر: پروتکل EAP-TLS ۱**
		شماره مؤلفه: رز-پا-ل‌ا-(ت‌س).۶,۱ (FCS_IPSEC_EXT.1.6)
		شرح مؤلفه:
		توابع امنیتی هدف ارزیابی باید به سرپرست مجاز اجازه دهند تا لیست مجموعه الگوریتم‌هایی را که ممکن است پیشنهاد شود و در طول تبادلات EAP-TLS پذیرفته شوند پیکربندی کند.
		نکته کاربردی:
		دنباله رمزهایی که در پیکربندی ارزیابی می‌شوند، توسط این الزام محدود شده‌اند. نویسنده هدف امنیتی باید دنباله رمزهای اختیاری را که پشتیبانی می‌شوند انتخاب کند، اگر دنباله رمز پشتیبانی شده‌ای به جز دنباله رمز الزامی وجود نداشته باشد، نویسنده هدف امنیتی باید «هیچکدام» را انتخاب کند. الگوریتم هایی که در اولین الزام این پروتکل (RFC 5430) لیست شده‌اند، الگوریتم‌های ارجح برای پیاده‌سازی هستند.

شماره	نام خانواده	عنصر امنیتی
الزام		
		در الزام رز-پا-ل-ا-(ت‌س).۴,۱ نیاز است که هدف ارزیابی بررسی‌های خاصی را بر روی گواهی‌نامه‌های ارائه شده توسط سرور احراز هویت انجام دهد، بررسی‌های مرتبطی وجود دارد که سرور احرازهویت بر روی گواهی‌نامه ارائه شده توسط کلاینت انجام خواهد داد. برای مثال فیلد extendedKeyUsage از گواهینامه کلاینت شامل «احراز هویت کلاینت» است و بیت توافقی کلید (برای دنباله رمز دیفی-هلمن) یا بیت رمزشده کلید (برای دنباله رمز RSA) تنظیم می‌شود. گواهینامه‌های به دست آمده برای استفاده توسط هدف ارزیابی با این الزام مطابق خواهد بود.
۱۸		**نام عنصر: تولید بیت تصادفی ۱** **شماره مؤلفه: رز-ب‌ت.۱,۱ (FCS_RBG.1.1)**
	تولید بیت تصادفی (ت‌س) **(FCS_RBG_EXT)**	**شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید تمام خدمات تولید بیت تصادفی را مطابق با [انتخاب: یکی از : NIST 800-90 با استفاده از Hash_DRBG (هرکدام), HMAC_DRBG(هرکدام)، CTR_DRBG (AES)، Dual_EC_DRBG (هرکدام)] ، پیوست C مربوط به FIPS Pub 140-2، پیوست ۲,۴ با استفاده از AES مربوط به X9.31] انجام دهد که توسط یک منبع آنتروپی انباشته از آنتروپی [انتخاب: یکی یا

شماره	نام خانواده	عنصر امنیتی
الزام		
		هر دو : منبع نویز مبتنی بر نرم‌افزار یا منبع نویز مبتنی بر سخت‌افزار توابع امنیتی هدف ارزیابی] جایگذاری شده است.
۱۹		**نام عنصر: تولید بیت تصادفی ۱**
		شماره مؤلفه: رز-ب‌ت.۲,۱ **(FCS_RBG_EXT.1.2)**
		شرح مؤلفه:
		تولید بیت تصادفی قطعی باید توسط کمینه‌ی [انتخاب، یکی از گزینه‌های ۱۲۸ یا ۲۵۶ بیت] آنتروپی با حداقل طول بیت مساوی یا بزرگتر از طول بیت کلیدها و پارامترهای احراز هویتی که تولید خواهدکرد، جایگذاری شود.
		نکته کاربردی :
		پیوست ث استاندارد NIST 800-90، کمینه آنتروپی اندازه‌گیری شده را که ممکن است در نسخه‌های آتی FIPS-140 مورد نیاز باشد، شرح می‌دهد. در نسخه‌های آتی این پروفایل حفاظتی مورد نیاز خواهد بود.
		برای اولین انتخاب در FCS_RBG_EXT.1.1، نویسنده هدف امنیتی باید استانداردی را که مطابق با خدمات RBG است، انتخاب کند.(یا NIST 800-90 یا پیوست ث از FIPS 140-2)، برای دومین انتخاب، نویسنده هدف امنیتی، نشان می‌دهد که چگونه کلاینت آنتروپی برای RBG را جمع‌آوری می‌کند.

شماره الزام	نام خانواده عنصر امنیتی

SP 800-90 چهار روش متفاوت برای تولید اعداد تصادفی را در برمی‌گیرد که هرکدام از اینها به نوبه خود به اصول اولیه رمزنگاری (توابع درهم‌ساز/رمز) بستگی دارد. نویسنده هدف امنیتی تابع مورد استفاده را انتخاب خواهد کرد(اگر 90-800 انتخاب شده‌باشد) و اصول اولیه رمزنگاری مشخص استفاده شده در الزامات یا در TSS را لحاظ می‌کند.

درحالی‌که هر کدام از توابع درهم‌ساز تعریف‌شده(SHA-1, SHA-224,SHA-256, SHA-384, SHA-512) برای Hash_DRBG یا HMAC_DRBG مجاز هستند، تنها پیاده‌سازی‌های مبتنی بر AES برای CT_DRBG مجازند.

هنگامی که هر کدام از منحنی‌های تعریف شده در 90-800 برای Dual_EC_DRBG مجاز هستند، نویسنده هدف امنیتی نه تنها باید منحنی انتخاب شده را لحاظ کند، بلکه باید الگوریتم درهم‌ساز استفاده شده را نیز لحاظ کند.

توجه داشته باشید که برای پیوست ث FIPS 140-2، در حال حاضر تنها روش شرح داده‌شده در توصیه‌ی NIST، تولید کننده عدد تصادفی مبتنی بر پیوست الف.۲,۴ از ANSI X9.31 با استفاده از ۳ کلید سه‌تایی الگوریتم‌های DES و AES در بخش ۳، معتبر است.

در اینجا اگر طول کلید استفاده شده در پیاده‌سازی AES متفاوت با آنچه که در رمزبندی داده‌ی کاربر به‌کار رفته‌است، باشد، آنگاه FCS_COP.1 باید برای برگرداندن طول کلید متفاوت، مجدداً تنظیم یا تکرار شود.

با انتخاب FCS_RBG_EXT.1.2، نویسنده هدف امنیتی کمینه عدد بیت‌های آنتروپی را که برای جادادن RBG استفاده شده است،

شماره	نام خانواده	عنصر امنیتی
الزام		

برمی‌گزیند.

نویسنده هدف امنیتی هم‌چنین اطمینان حاصل می‌کند که تمام توابع اصلی در الزامات پایه‌ای برای هدف ارزیابی گنجانده شده‌اند.

در آینده بیشتر الزامات شرح داده شده در «روشی برای آزمودن منبع آنتروپی: الزامات و شرح مجموعه آزمون» برای این پروفایل حفاظتی مورد نیاز خواهند بود.

۶,۳ کلاس حفاظت از داده‌های کاربری

در ادامه المان‌های 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 می‌نمایند: 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 نشان می-دهند.

خانواده‌های این کلاس در چهار گروه زیر دسته بندی شده‌اند:

۱) سیاست‌های امنیتی مربوط به محافظت از داده کاربری

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

در این دو خانواده به نویسنده هدف امنیتی/پروفایل حفاظتی اجازه داده می‌شود تا سیاست‌های امنیتی را که برای حفاظت از داده‌کاربری در نظر گرفته شده‌اند و همچنین حوزه کنترلی این سیاست‌ها را نام ببرد.
سیاست‌های امنیتی نام برده شده در این دو خانواده

- سیاست‌های امنیتی در نظر گرفته شده برای کنترل دسترسی
- سیاست‌های 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)[3] و توابع کنترل جریان اطلاعات (حف-کج)[4] قوانینی که تعریف کننده‌ی «سیاست‌های امنیتی کنترل دسترسی» و «سیاست‌های امنیتی کنترل جریان اطلاعات» هستند، آورده شده است.

۲) فرم‌های مختلف محافظت از داده کاربری

- توابع کنترل دسترسی (حف-ت‌ک)

---

1 Access control policy(FDP_ACC)
2 Information flow control policy(FDP_IFC)
3 Access control functions(FDP_ACF)
4 Information flow control functions(FDP_IFF)

- توابع کنترل جریان اطلاعات (حف-ک‌ج)
- انتقال داخلی در هدف ارزیابی (حف-اد)[1]
- حفاظت از اطلاعات باقیمانده (حف-اب)[2]
- عملیات عقب‌گرد به منظور بازگرداندن حالت/حالت‌های قبل (حف-ع‌گ)[3]
- یکپارچگی داده‌های ذخیره شده (حف-ی‌د)[4]

۳) ورود و خروج، ذخیره‌سازی برون‌خطی[5]

- احراز هویت[6] داده (حف-ت‌د)
- صادر شده از هدف ارزیابی (حف-ص‌ا)[7]
- ورود داده‌ها از بیرون به هدف ارزیابی (حف-وب)[1]

---

1 Internal TOE transfer(FDP_ITT)

2 Residual information protection(FDP_RIP)

3 Rollback(FDP_ROL)

4 Stored data integrity(FDP_SDI)

5 Offline

6 Data authentication(FDP_DAU)

7 Export from the TOE(FDP_ETC)

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

۴) ارتباطات میان توابع امنیتی هدف ارزیابی

- محافظت از انتقال محرمانگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(ح‌ف-م‌د)[۲]
- محافظت از انتقال یکپارچگی داده کاربر توابع امنیتی هدف ارزیابی داخلی(ح‌ف-ی‌ا)[۳]

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

➢ خانواده سیاست‌های کنترل دسترسی

این خانواده سیاست‌های 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[۴] تحت کنترل سیاست‌گذاری‌ها
- موجودیت‌های غیرفعال[۵] تحت کنترل سیاست‌گذاری‌ها
- عملیات بین موجودیت‌های فعال کنترل شده و موجودیت‌های غیرفعال کنترل شده که توسط سیاست‌های امنیتی پوشش داده می‌شود.

---

1 Import from outside of the TOE(FDP_ITC)

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

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

4 Subject

5 Object

بنابراین در مؤلفه‌های این خانواده، سیاست امنیتی نام برده می‌شود و برای هریک از سیاست‌های امنیتی نامبرده، موجودیت فعال و غیرفعال تحت کنترل آن سیاست و عملیات بین موجودیت فعال و غیرفعال نیز نام برده می‌شود.

در این خانواده می‌توان سیاست‌های 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 سیاست‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-س‌ک.۱,۱(۱)، حف-س‌ک.۱,۱(۲)).

قوانینی که عملکرد سیاست‌های امنیتی را برای کنترل دسترسی تعریف می‌نمایند در خانواده‌های توابع کنترل دسترسی (حف-ت‌ک) و صادر شده از هدف ارزیابی (حف-ص‌ا) تعریف می‌شوند.

سیاست‌های 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 سیاست‌های امنیتی کنترلی دسترسی (حف-س‌ک)، تنها این سیاست‌ها نام برده می‌شوند، اما در این خانواده قوانینی برای اجرای سیاست 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 سیاست‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام برده می‌شوند.

➢ خانواده احراز هویت داده

احراز هویت داده به هر نهادی، اجازه‌ی پذیرش مسوولیت احراز صحت اطلاعات را می‌دهد (با دیجیتالی امضاء کردن 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) سیاست‌های امنیتی بر روی کنترل دسترسی و جریان اطلاعات نام برده شده‌اند. در این خانواده این سیاست‌های امنیتی بر روی داده تحت کنترل این سیاست‌ها 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.

➢ سیاست‌های 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 سیاست‌ها هستند.

بنابراین در مؤلفه‌های این خانواده، سیاست امنیتی نام برده می‌شوند و برای هریک از سیاست‌های امنیتی نام برده شده، موجودیت فعال و غیرفعال تحت کنترل آن سیاست و عملیات بین موجودیت فعال و غیرفعال نیز نام برده می‌شوند.

در این خانواده می‌توان سیاست‌های 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 سیاست‌های امنیتی به صورت جداگانه تکرار شود (به طور مثال حف-خج.۱,۱(۱)، حف-خج.۱,۱(۲)).

قوانینی که عملکرد سیاست‌های امنیتی را برای کنترل دسترسی تعریف می‌نمایند، در خانواده‌های توابع کنترل دسترسی (حف-کج) و صادر شده از هدف ارزیابی (حف-صا) تعریف می‌شوند.

سیاست‌های 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 سیاست‌های امنیتی کنترلی دسترسی (حف-خج)، تنها این سیاست‌ها نام برده می‌شوند اما در این خانواده قوانینی برای اجرای سیاست 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 سیاست‌های امنیتی و مشخصه‌های امنیتی مربوط به آنها نام برده می‌شوند.این خانواده شامل دو الزام است:

- 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 تعامل است. با توجه به ماهیت آنها سرپیچی از سیاست‌گذاری‌های امنیتی مربوط به کنترل جریان اطلاعات، منجر به نقص در سیاست‌ها می‌شود. بنابراین، باید عملیات خاصی برای جلوگیری یا محدود کردن 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 سیاست‌های امنیتی (سیاست‌های امنیتی کنترل جریان و کنترل دسترسی) خارج از هدف ارزیابی است. برای ورود داده باید سیاست‌های تعریف شده بر روی داده اعمال شود، هم‌چنین مشخصه های امنیتی مطلوبی برای این‌گونه داده‌ها در نظر گرفته می‌شود. در واقع این خانواده محدودیت‌هایی بر روی داده‌های ورودی خارج از 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 را براساس مشخصه‌های امنیتی از یکدیگر مجزا کند 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 کردن 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.

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

1 Internal channel

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، تامین 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
۲۰	حفاظت از داده های باقی مانده (FDP_RIP)	**نام عنصر: حفاظت کامل از داده‌های 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، آزادسازی منابع از] تمام موجودیت های غیرفعال، غیرقابل دسترس کنند.

۶,۴ کلاس شناسایی و احراز هویت

نام کلاس: ممیزی امنیت

شرح کلاس: سامانه‌های تشخیص نفوذ برای رخدادهای گوناگون اقدام به ایجاد گزارشهایی برای ممیزی می‌کنند. کلاس ممیزی امنیت، الزاماتی پیرامون نحوه شناخت، ثبت، ذخیره و تحلیل اطلاعات ممیزی مربوط به فعالیت‌های مرتبط امنیتی تعریف می‌کند (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 سیستم در برخورد با خطاهای امنیتی[1]**

این خانواده تعریف کننده الزامات برای واکنش‌های سیستم 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 را که بایستی توسط توابع امنیتی هدف ارزیابی قابل ممیزی باشند 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.

1 Security audit automatic response (FAU_ARP)

2 Security audit data generation (FAU_GEN)

- **خانواده تحلیل ممیزی امنیت[1]**

این خانواده الزاماتی برای ابزارهای خودکار، که فعالیت‌های سیستم 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]**

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

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)

شماره الزام	نام خانواده	عنصر امنیتی
۲۱	پروتکل 802.1X (FIA_8021X_EXT)	**نام عنصر: احرازهویت موجودیت دسترسی به پورت 802.1X ۱** **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 دسترسی به پورت (PAE) نقش «درخواست کننده» داشته 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 می‌کند (یا دیگر تبادلات EAP مناسب) و یک دستدهی [1]چهار طرفه با سیستم دسترسی بی‌سیم انجام می‌دهد (احراز کننده) تا ارتباط 802.11 شروع شود.

همان‌طور که پیشتر نشان داده شد، حداقل دو مسیر ارتباطی در طول تبادل وجود دارد، یکی با

1 Handshake

شماره الزام	نام خانواده	عنصر امنیتی
		سیستم دسترسی بی‌سیم و دیگری با سرور احراز هویت که از سیستم دسترسی بی‌سیم به صورت رله استفاده می‌کند. هدف ارزیابی یک EAP بر روی اتصال LAN با سیستم دسترسی بی‌سیم به صورت مشخص شده در 802.1X-2010 ایجاد می‌کند. هدف ارزیابی و سرور احراز هویت یک نشست EAP-TLS برقرار می‌کند (RFC 5216). نکته‌ی انجام احرازهویت 801.1X به‌دست آوردن دسترسی به شبکه است(با فرض اینکه احراز هویت موفق بوده است و تمام مذاکرات 802.11 موفقیت آمیز بوده‌اند. در مجموعه اصطلاحات 802.1X این به این معنی است که هدف ارزیابی دسترسی به « پورت کنترل شده» نگهداری شده توسط سامانه دسترسی بی‌سیم را به دست خواهد آورد.)
۲۲	گواهینامه X509 (FIA_X509_EXT)	**نام عنصر: گواهینامه X509 ۱** **شماره مؤلفه: اش-X509.۱،۱ (FIA_X509_EXT .1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید از گواهینامه X.509v3 به صورت تعریف شده توسط RFC 5280 استفاده کند

شماره الزام	نام خانواده عنصر امنیتی	
		تا از احراز هویت برای تبادلات EAP-TLS پشتیبانی کنند.

نکته کاربردی:

باید توجه شود که RFC 5280 الزاماتی برای اعتبارسنجی گواهی‌نامه و الزامات اعتبارسنجی مسیر گواهی-نامه تعریف کرده است که باید توسط هدف ارزیابی به عنوان هر یک بخش از این الزام، پیاده‌سازی شود.

۶,۵ 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، 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. هـم-چنین در این کلاس می‌توان نقش‌های مدیریتی مختلف، تعاملات آنها از جمله جداسازی قابلیت‌های هر نقش را مشخص کرد.

از اهداف این کلاس می‌توان به موارد زیر اشاره کرد:

- 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 مشخصه‌های 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]

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

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.

- **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 است.

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

این خانواده اجازه می‌دهد تا عملکردهای مدیریتی ارائه شده توسط هدف ارزیابی مشخص شود. عملکردهای مدیریتی با فراهم کردن رابط توابع امنیتی هدف ارزیابی[4]، به سرپرستان اجازه می‌دهند تا پارامترهایی 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.

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

➢ خانواده نقش‌های مدیریت امنیتی[1]

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.

شماره الزام	نام خانواده	عنصر امنیتی
۲۳	خانواده مشخصات کارکردهای مدیریتی **(FMT_SMF)**	**نام عنصر: مشخصات کارکردهای مدیریتی ۱** **شماره مؤلفه: م‌د-ع‌م.۱،۱ (FMT_SMF.1.1)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید توانایی اجرای کارکردهای مدیریتی زیر را داشته باشد: • مشخص کردن CA که توسط آن هدف ارزیابی، گواهی‌نامه‌های سرور احرازهویت را می‌پذیرد. • مشخص کردن FQDN از گواهی‌نامه‌های سرور احراز هویت قابل پذیرش • فعال/غیرفعال کردن چک لیست‌های ابطال گواهی‌نامه • پیکربندی زمان بازه زمانی ارسال و دریافت رمز برای کلیدهای نشستی که برقرار شده است. واحد

1 Security management roles (FMT_SMR)

شماره الزام	نام خانواده	عنصر امنیتی

اندازه گیری برای این بازه زمانی بیشتر از یک ساعت نباید پیکربندی شود.

- غیرفعال کردن قابلیت اتصال کلاینت به کلاینت بی‌سیم ad hoc
- غیرفعال کردن قابلیت پل‌زدن شبکه بی‌سیم
- غیرفعال کردن قابلیت رومینگ
- مشخص کردن مجموعه الگوریتم‌هایی که ممکن است در طول تبادل EAP-TLS پیشنهاد شود یا پذیرفته شود.
- مشخص کردن شبکه‌های بی‌سیم که برای متصل شدن هدف ارزیابی، قابل قبول هستند.
- توانایی فعال/غیرفعال کردن IEEE 802.1X پیش از احراز هویت
- توانایی فعال/غیرفعال کردن و پیکربندی PMK ذخیره شده:
  - تنظیم میزان زمانی که موجودیت PMK ذخیره شده است.
  - تنظیم بیشترین تعداد موجودیت PMK که ذخیره شده است.
- توانایی به روزرسانی هدف ارزیابی و بررسی به روزرسانی‌ها

شماره الزام	نام خانواده	عنصر امنیتی

- توانایی پیکربندی تمام کارکردهای مدیریت امنیتی معرفی شده در دیگر بخش‌های این پروفایل حفاظتی
- [اختصاص: هر کارکرد مدیریتی دیگر]

نکته کاربردی:

برای نصب، کلاینت WLAN جهت احراز سرپرست ماشین کلاینت، به محیط IT متکی است. برای کارکرد پیکربندی بازه زمانی ارسال و دریافت کلیدهای نشست برقرار شده، واحد اندازه‌گیری باید بیش از یک ساعت نباشد. برای مثال: واحد اندازه‌گیری ثانیه، دقیقه و ساعت قابل قبول است و واحد اندازه‌گیری روز و بیشتر از آن غیرقابل قبول است.

۶,۶ 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 می‌باشند. 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 سیاست‌های 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 هستند.
- 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 می‌کند در زمان رخ دادن شکست، عملکرد امنیتی هدف ارزیابی در وضعیت امن نگهداشته شود.

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

1 Bypass

2 Fail secure(FPT_FLS)

3 Availability of exported TSF data(FPT_ITA)

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 داده-ها، 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.

- **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 می‌کند که از داده توابع امنیتی هدف ارزیابی در زمان انتقال بین بخش‌های مجزای توابع امنیتی هدف ارزیابی در سراسر کانال داخلی محافظت می‌کند.

---

1 Confidentiality of exported TSF data (FPT_ITC)

2 Integrity of exported TSF data (FPT_ITI)

3 Internal TOE TSF data transfer (FPT_ITT)

➢ خانواده محافظت فیزیکی از توابع امنیتی هدف ارزیابی[1]

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.

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 می‌دهد که توابع امنیتی هدف ارزیابی چگونه باید به تلاش‌هایی که در ارتباط با تداخل فیزیکی صورت می‌گیرد واکنش نشان دهند.

➢ خانواده بازیابی مطمئن[2]

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 راه اندازی شود. این خانواده بسیار مهم است زیرا وضعیت راه‌اندازی توابع امنیتی هدف ارزیابی، تعیین کننده‌ی حفاظت از وضعیت‌های بعدی است.

➢ خانواده تشخیص تکرار[3]

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

---

1 TSF physical protection (FPT_PHP)

2 Trusted recovery (FPT_RCV)

3 Replay detection (FPT_RPL)

➢ خانواده پروتکل هم‌زمانی حالت[1]

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.

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[2]

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

➢ خانواده هم‌خوانی داده‌های بین توابع امنیتی هدف ارزیابی[3]

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 اشتراک‌گذاری 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[4]

1 State synchrony protocol (FPT_SSP)

2 Time stamps (FPT_STM)

3 Inter-TSF TSF data consistency

4 Testing of external entities(FPT_TEE)

این خانواده الزاماتی را برای توابع امنیتی هدف ارزیابی تعریف می‌کند 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، سیستم‌عامل و ...) یا برنامه‌ها و باکس‌های متصل شده به هدف ارزیابی (سیستم‌های تشخیص نفوذ، فایروال‌ها، سرورهای ورود، سرورهای زمانی و غیره) باشد.

➢ 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 داده ها، یکسان بودن داده ها 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 شبکه ای، 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 عملیات ریاضی مثالی از این الزام است. این‌گونه آزمون‌ها می‌توانند در هنگام راه اندازی، به طور متناوب بنا به درخواست کاربر مجاز، یا در زمانی‌که شرایط خاصی ایجاد شود، انجام گیرند. عملی که باید به عنوان نتیجه خودآزمایی توسط هدف ارزیابی انجام شود در دیگر خانواده‌ها تعریف می‌شود.

---

1 Internal TOE TSF data replication consistency(FPT_TRC)

2 TSF self test(FPT_TST)

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 را (که توسط دیگر خانواده‌ها اداره شده‌اند) متوقف نمی‌کنند، مورد نیاز است.
چنین خرابی‌هایی می‌توانند یا به دلیل حالت‌های پیش‌بینی نشده خرابی یا سهل‌انگاری‌های مرتبط با طراحی سخت‌افزار، میان‌افزار یا نرم افزار رخ دهند و یا به دلیل تغییر مخرب توابع امنیتی هدف ارزیابی بر اثر حفاظت منطقی و/یا فیزیکی ناکافی صورت گیرند.

شماره	نام خانواده	عنصر امنیتی
الزام		
۲۴	خودآزمایی توابع امنیتی هدف ارزیابی (FPT_TST)	**نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی۱** **شماره مؤلفه: ح‌ت-خ‌ا-(ت‌س).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.
۲۵		**نام عنصر: خودآزمایی توابع امنیتی هدف ارزیابی۱** **شماره مؤلفه: ح‌ت-خ‌ا-(ت‌س).۲,۱ (FPT_TST_EXT.1.2)** **شرح مؤلفه:**

شماره	نام خانواده	عنصر امنیتی
الزام		
		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 توابع امنیتی هدف ارزیابی، بررسی و راستی آزمایی شوند.
		نکته کاربردی:
		در حالیکه هدف ارزیابی معمولاً بسته نرم‌افزاری می‌باشد که در محیط IT اجرا می‌شود، با این وجود قادر به انجام فعالیت‌های خودآزمایی ضروری بالا می‌باشد. قابل درک است که در ارزیابی اطمینانی که آزمون‌های ذکر شده در بالا ارائه کرده‌اند، وابستگی معناداری به محیط میزبان وجود دارد(بدین معنا که اگر محیط میزبان به خطر افتد، خودآزمایی بی‌معنی خواهد بود).
۲۶	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

شماره الزام	نام خانواده عنصر امنیتی
	افزار هدف ارزیابی را پرس و جو و مشاهده نمایند.
۲۷	**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.
۲۸	**نام عنصر: به روز رسانی امن ۱**
	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.

شماره	نام خانواده	عنصر امنیتی
الزام		

نکته کاربردی:

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

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

۶,۷ کلاس دسترسی به هدف ارزیابی

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

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

این خانواده الزاماتی را تعریف می‌کند تا دامنه‌ی صفات و ویژگی‌های امنیتی نشست را که یک کاربر 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.

1 Limitation on scope of selectable attributes(FTA_LSA)

2 Limitation on multiple concurrent sessions(FTA_MCS)

➢ قفل کردن و خاتمه دادن نشست[1]

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[2]

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

➢ سوابق دسترسی به هدف ارزیابی[3]

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 دسترسی به حساب کاربری را به کاربر نمایش دهد.

➢ برقراری نشست هدف ارزیابی[4]

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

شماره الزام	نام خانواده عنصر امنیتی

1 Session locking and termination(FTA_SSL)

2 TOE access banners(FTA_TAB)

3 TOE access history(FTA_TAH)

4 TOE session establishment(FTA_TSE)

شماره الزام	نام خانواده عنصر امنیتی
۲۹	برقراری نشست بی-سیم (FTA_WSE_EXT)

نام عنصر: برقراری نشست بی‌سیم ۱

شماره مؤلفه: دس-ب‌ن-(ت‌س).۱,۱ (FTA_WSE_EXT.1.1)

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید تنها تلاش کنند تا به شبکه بی‌سیمی که به عنوان یک شبکه قابل قبول براساس [اختصاص: مشخصه‌هایی جهت شناسایی لیستی از شبکه‌های قابل قبول] که توسط سرپرست مجاز پیکربندی شده است، متصل شود.

نکته کاربردی:

منظور این الزام آن است که به سرپرست اجازه دهد تا نقاط دسترسی را به آنچه که هدف ارزیابی مجاز است متصل شود، محدود کند. قسمت «اختصاص» توسط نویسنده هدف امنیتی استفاده می‌شود تا ویژگی-هایی را که می‌تواند توسط سرپرست جهت مشخص کردن نقاط دستیابی قابل قبول استفاده‌شود، مشخص کند.

۶,۸ 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 دستورات 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]**

1 Inter-TSF trusted channel(FTP_ITC)

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 کارآیی 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[1]

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.

شماره الزام	نام خانواده	عنصر امنیتی
۳۰	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 EAP-TLS کانال ارتباطی امنی بین خود و نقطه دسترسی بی‌سیم ارائه کند که به طور منطقی از دیگر کانال‌های ارتباطی جدا است و

1 Trusted path(FTP_TRP)

شماره	نام خانواده الزام	عنصر امنیتی
		به صورت مطمئن نقطه پایانی‌اش را شناسایی می‌کند و از داده‌های کانال در برابر تغییر یا افشاء، محافظت می‌کند.
۳۱		**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 مورداعتماد را به خود بدهد.
۳۲		**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 مورد اعتماد پیش از هر ارتباط دیگری از طریق شبکه متصل شده شروع کنند. **نکته کاربردی:**

شماره نام خانواده

الزام

عنصر امنیتی

منظور الزام بالا استفاده از پروتکل رمزنگاری معرفی شده در الزام، جهت محافظت از ارتباطات هدف ارزیابی با نقطه دسترسی می‌باشد.

این الزام نشان می‌دهد که ارتباط محافظت شده نه تنها در زمان برقراری ارتباط ایجاد می‌شود، بلکه پس از قطعی، ارتباط محافظت شده دوباره از سر گرفته می‌شود. در مواردی که بخشی از تنظیمات هدف ارزیابی، به صورت دستی تونل‌ها را جهت حفاظت ارتباطات دیگر راه‌اندازی می‌کند و چنان‌چه پس از قطعی ارتباط، هدف ارزیابی سعی در برقراری مجدد ارتباط به صورت خودکار یا مداخله دستی می‌کند، ممکن است فرصتی ایجاد شود که مهاجم قادر به دستیابی به اطلاعات بحرانی شود یا اتصال به خطر افتد.

نام کلاس	نام عناصر تضمین	توضیحات
Development	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents	AGD_OPE.1	راهنمای کاربری عملیاتی
	AGD_PRE.1	راهنمای کاربری آماده‌سازی

Tests	ATE_IND.1	آزمون مستقل- انطباق
Vulnerability Assessment	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support	ALC_CMC.1	برچسب گذاری هدف ارزیابی
	ALC_CMS.1	پوشش مدیریت پیکربندی هدف ارزیابی

۷ کلاس توسعه

۷,۱ مشخصات کارکردی

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۱	مشخصات کارکردی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه دهنده باید مشخصات کارکردی را ارائه کند.
۲		**نام عنصر: مشخصات کارکرد ابتدایی۱**

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	نام خانواده	عنصر امنیتی
		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، می‌باشند. با توجه به دلایلی که باید در مستندات و بخش "خلاصه مشخصات هدف ارزیابی" وجود داشته باشند، الزامات کارکردی تضمین می‌گردند. 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)** **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]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

[1] SFR-enforcing TSFI

[2] SFR-supporting TSFI

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		کننده‌ی الزام کارکرد امنیتی را مشخص کند.
۵		**نام عنصر: مشخصات کارکرد ابتدایی۱** **شماره مؤلفه: (ADV_FSP.1.3C)** **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 می‌کند.
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 می-باشند.

۷,۲ کلاس راهنمای کاربر

۷,۲,۱ 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 می‌گردد.
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 نموده 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 مدهای عملیاتی هدف ارزیابی (مدهایی شامل شکست عملیات یا خطای عملیات)، آثار آنها و مستلزم بودنشان برای حفظ عملیات در حالت امن را مشخص نمایند.
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 گردند.
۱۶		**نام عنصر: راهنمای کاربردی ۱** **شماره مؤلفه: (AGD_OPE.1.7C)** **شرح مؤلفه:**

مؤلفه‌های محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
		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.

۷,۲,۲ 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:** 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 نمایند.

مؤلفه‌های اقدامات محتوایی		
شماره الزام	نام خانواده	عنصر امنیتی
۲۰		**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.2C)** **شرح مؤلفه:** 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 نمایند.

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**

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

۷,۳ کلاس آزمون

آزمون هدف ارزیابی برای بررسی کارکرد سیستم و جنبه‌هایی که از ضعف طراحی و پیاده‌سازی سود می‌برند، در نظر گرفته می‌شود. آزمون کارکردی سیستم 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 می‌گردد. یکی از خروجی‌های اولیه پروسه ارزیابی گزارش آزمون می‌باشد که در الزامات زیر مشخص شده است.

۷,۳,۱ 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 می‌کند و ارزیاب گزارشی از طرح آزمون و نتایج آن آماده می‌کند.

مؤلفه‌های اقدامات توسعه دهنده		
شماره الزام	**نام خانواده**	**عنصر امنیتی**
۲۳	آزمون مستقل **(ATE_IND)**	**نام عنصر: آزمون مستقل ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه دهنده باید برای آزمودن ، هدف ارزیابی را 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 آزمودن 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 بیازماید تا تائید کند که توابع امنیتی هدف ارزیابی به صورت مشخص شده عمل می‌کنند.

۷,۴ کلاس آسیب‌پذیری

برای آماده نمودن اولیه این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه‌های ارزیابی با تحلیل هدف ارزیابی آن دسته از آسیب‌پذیری‌هایی که در این نوع محصولات یافت شده‌اند بیابد. 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 گردد. اینگونه اطلاعات در توسعه ابزارهای آزمون نفوذ و همچنین نسخه‌های بعدی پروفایل‌های حفاظتی مورد استفاده قرار خواهند گرفت.

۷,۴,۱ 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 آزمودن، 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 آزمودن 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.

مؤلفه‌های اقدامات ارزیاب		
شماره الزام	نام خانواده	عنصر امنیتی
۳۰		**نام عنصر: آسیب‌پذیری ۱** **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.

۷,۵ 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 می‌گردد 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.

۷,۵,۱ قابلیت‌های پیکربندی

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

۷,۵,۲ 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..

۸ پیوست الف

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

***

۸,۱ کلاس: ممیزی امنیت (م‌ا)

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 الزام	نام خانواده	عنصر امنیتی
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 دسترسی 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)**

شماره	نام خانواده	عنصر امنیتی	الزام
		شرح مؤلفه:	
		توابع امنیتی هدف ارزیابی باید رکوردهای ممیزی را به صورت مناسبی به سرپرستان مجاز ارائه دهد تا اطلاعات را تفسیر نمایند.	
۴۱		**نام عنصر: بازبینی ممیزی محدود ۲**	
		شماره مؤلفه: م۱-ب‌ز.۱,۲ (FAU_SAR.2.1)	
		شرح مؤلفه:	
		توابع امنیتی هدف ارزیابی باید مانع تمام کاربران به جز سرپرستان مجاز از داشتن دسترسی خواندن به رکوردهای ممیزی در دنباله ممیزی شوند.	
۴۲	بازبینی ممیزی محدود شده (FAU_STG)	**نام عنصر: جلوگیری از فقدان داده ممیزی ۱**	
		شماره مؤلفه: م۱-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	

شماره	نام خانواده
الزام	

عنصر امنیتی

بیش از یک اقدام زیر را انتخاب کنند:

الف- جلوگیری از رویدادهای قابل ممیزی، به جز رویدادهایی که توسط کاربر مجاز صورت گرفته‌اند.

ب- رونویسی رکوردهای ممیزی که قبلاً ذخیره شده‌اند.

نکته کاربردی:

هدف ارزیابی باید برای سرپرستان مجاز، گزینه‌ای را ارائه دهد تا بتوانند از ممیزی داده‌های از دست رفته با جلوگیری از وقوع رویدادهای قابل ممیزی، جلوگیری کنند. لزومی ندارد اقدامات سرپرستی مجاز تحت این شرایط ممیزی شود. هدف ارزیابی هم‌چنین به سرپرستان مجاز گزینه‌ای ارائه می‌دهد تا به جای آنکه از رویدادهای قابل ممیزی جلوگیری کنند، رکوردهای ممیزی قدیمی را رونویسی کنند که از آن در برابر حملات منع خدمت [1]محافظت کند.

1 Denial of Service(DoS)

۸,۲ کلاس شناسایی و احراز هویت

در مواردی که هدف ارزیابی قابلیت سرپرستی را ارائه می‌دهد، الزاماتی وجود دارد که برای مشخص کردن آن قابلیت می‌تواند به کار برود، همانند سرپرستی راه‌دور، سرپرستی محلی و حفاظت از نشست سرپرستی. برای این نسخه از پروفایل حفاظتی، استفاده از الزامات سرپرستی از پروفایل حفاظتی سیستم دسترسی بی‌سیم[1] قابل قبول است تا قابلیت‌هایی را برای کلاینت مشخص کند.

در برخی موارد هدف ارزیابی قابلیت‌هایی را جهت ذخیره و مدیریت گواهی‌نامه‌های استفاده شده در طول تبادل استفاده می‌کند، الزامات زیر می‌تواند در هدف امنیتی در نظر گرفته شود:

شماره الزام	نام خانواده	عنصر امنیتی
۴۳	گواهینامه‌های X509 (FIA_X509_EXT)	**نام عنصر: مدیریت و ذخیره گواهی‌نامه‌های X509 ۲** **شماره مؤلفه: اش-X509.۲,۲ (FIA_X509.2.2)** **شرح مؤلفه:** توابع امنیتی هدف ارزیابی باید گواهی‌نامه‌ها را ذخیره و از حذف و تغییر غیرمجاز محافظت کند.
۴۴		**نام عنصر: مدیریت و ذخیره گواهینامه‌های X509 ۲** **شماره مؤلفه: اش-X509.۳,۲ (FIA_X509.2.3)**

1 Wireless Access System

شماره نام خانواده

الزام

عنصر امنیتی

شرح مؤلفه:

توابع امنیتی هدف ارزیابی باید قابلیتی را برای سرپرستان مجاز فراهم کند تا گواهینامه‌های X.509v3 را در داخل هدف ارزیابی برای استفاده توسط توابع امنیتی مشخص شده در این پروفایل حفاظتی بارگذاری کند.

نکته کاربردی:

اش-X509.(تس).۲,۱.۱ به گواهی‌نامه‌هایی که توسط توابع امنیتی هدف ارزیابی استفاده می‌شوند اعمال می‌شود. نیازی نیست گواهی‌نامه‌هایی که توسط دیگر مؤلفه‌های در محیط عملیاتی استفاده و پردازش شده‌اند، توسط این مؤلفه پوشش داده شود.

۸,۳ الزامات ممیزی

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

الزام	رویدادهای قابل ممیزی	محتویات رکورد ممیزی اضافی
ما-ب‌ز.۱ FAU_SAR.1	هیچ	

ما-ب‌ز.۲	FAU_SAR.2	تلاش جهت خواندن رکوردهای ممیزی	هیچ
ما-ذخ.(ت‌س).۴	FAU_STG_EXT.4	رسیدن دنباله ممیزی به ظرفیت	هیچ
اش509X.(ت‌س).۲	FIA_X509_EXT.2	تلاش جهت بارگذاری گواهی‌نامه‌ها تلاش جهت ابطال گواهی‌نامه‌ها	هیچ