به نام خدا

پروفایل حفاظتی سیستم‌های عامل همه‌منظوره

دی ۹۴

نسخه ۱,۰

فهرست مطالب

۱- مقدمه ۵
۲- فرهنگ اصطلاحات ۵
۲-۱-اصطلاحات معیار مشترک ۵
۲-۲-اصطلاحات تکنولوژی ۷
۳- شرح محصول ۱۱
۳-۱-مرزهای محصول ۱۱
۳-۲-سکو محصول ۱۱
۳-۳-حالت‌های استفاده ۱۲
۴- مسائل امنیتی ۱۳
۴-۱-کلیات ۱۳
۴-۲-تهدیدات ۱۳
۴-۳-مفروضات ۱۴
۵- اهداف امنیتی ۱۵
۵-۱-کلیات ۱۵
۵-۲-اهداف امنیتی برای محصول ۱۶
۵-۳-اهداف امنیتی برای محیط عملیاتی ۱۹
۵-۴-منطق اهداف امنیتی ۲۰

۶- الزامات کارکرد امنیتی ۲۲
۶-۱- قراردادها ۲۲
۶-۲- کلاس پشتیبانی رمزنگاری ۲۵
۶-۳- کلاس حفاظت از داده کاربر ۳۶
۶-۴- کلاس مدیریت امنیت ۳۹
۶-۵- کلاس حفاظت از توابع هدف امنیتی ۴۱
۶-۶- کلاس تولید داده ممیزی ۴۴
۶-۷- کلاس شناسایی و احراز هویت ۴۶
۶-۸- کلاس کانال‌ها یا مسیرهای قابل‌اعتماد ۴۹
۷- الزامات تضمین امنیت ۵۱
۷-۱- کلاس ارزیابی هدف امنیتی (ASE) ۵۳
۷-۲- کلاس توسعه (ADV) ۵۳
۷-۳- کلاس مستندات راهنما (AGD) ۵۷
۷-۴- کلاس پشتیبانی چرخه حیات (ALC) ۶۴
۷-۵- کلاس آزمون‌ها (ATE) ۷۳
۷-۶- کلاس ارزیابی آسیب‌پذیری (AVA) ۷۷
۸- اقدامات تضمین الزامات کارکرد امنیتی ۸۱
پیوست ۱ الزامات اختیاری ۱۲۹
۱- کلاس پشتیبانی رمزنگاری ۱۲۹
۲- کلاس دسترسی به هدف ارزیابی ۱۳۰

پیوست ۲ الزامات مبتنی بر انتخاب..... ۱۳۲
۱- کلاس پشتیبانی رمزنگاری..... ۱۳۲
پیوست ۳ الزامات هدف..... ۱۳۵
۱- کلاس پشتیبانی رمزنگاری..... ۱۳۵
۲- کلاس حفاظت از توابع هدف امنیتی ۱۳۶
پیوست ۴ الزامات برآورده شده ذاتی..... ۱۴۱
پیوست ۵ مستندسازی آنتروپی و ارزیابی..... ۱۴۳
توصیف طراحی ۱۴۳
استدلال آنتروپی..... ۱۴۴
شرایط عملیات..... ۱۴۵
آزمون سلامت..... ۱۴۵
پیوست ۶ واژگان اختصاری ۱۴۶
پیوست ۷ مراجع ۱۵۰

۱- مقدمه

این سند که در راستای ارزیابی امنیتی محصولات مبتنی بر معیار مشترک توسط مرکز مدیریت راهبردی افتا و سازمان فناوری اطلاعات ایران تهیه و نهایی شده است، برای بیان الزامات کارکرد امنیتی هر محصول لازم است. بیان این الزامات برای توسعه‌دهندگان 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 خواهد کرد.

دامنه کاربرد این پروفایل حفاظتی (PP) برای توصیف قابلیت کارکردی امنیتی سیستم‌عامل‌ها از دیدگاه معیار مشترک (CC) و تعریف الزامات کارکردی و تضمین برای چنین محصولاتی می‌باشد. یک سیستم‌عامل، نرم‌افزاری است که منابع سخت‌افزاری و نرم‌افزاری کامپیوتر را مدیریت کرده و خدمات مشترکی برای برنامه‌های کاربردی فراهم می‌کند. سخت‌افزاری که سیستم‌عامل مدیریت می‌کند ممکن است فیزیکی یا مجازی باشد.

۲-فرهنگ اصطلاحات

۲-۱- اصطلاحات معیار مشترک

- **استاندارد ارزیابی معیار مشترک (CC)**

  استاندارد ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

- **متدولوژی ارزیابی معیار مشترک[1](CEM)**

  متدولوژی ارزیابی معیار مشترک برای ارزیابی امنیت فناوری‌های اطلاعات.

[1] Common Evaluation Methodology(CEM)

- **پروفایل حفاظتی[۲] (PP)**

مجموعه‌ای از الزامات امنیتی مستقل از پیاده‌سازی برای دسته‌ای از محصولات.

- **هدف امنیتی[۳] (ST)**

مجموعه‌ای از الزامات امنیتی وابسته به پیاده‌سازی برای یک محصول خاص.

- **هدف ارزیابی (TOE)**

محصول تحت ارزیابی، که در این مورد، محصول سیستم‌عاملی است که در بخش مرزهای محصول توضیح داده شده به همراه مستندات پشتیبانی‌کننده آن.

- **توابع هدف امنیتی[۴] (TSF)**

قابلیت‌های کارکردی امنیتی محصول تحت ارزیابی.

- **خلاصه مشخصه محصول[۵] (TSS)**

شرحی از نحوه برآوردن الزامات کارکرد امنیتی در یک هدف امنیتی توسط محصول.

---

[۲] Protection Profile

[۳] Security Target

[۴] TOE Security Functions (TSF)

[۵] TOE Summary Specification (TSS)

- **الزام کارکرد امنیتی[۶] (SFR)**

الزاماتی برای اجرای امنیت توسط محصول.

- **الزامات تضمین امنیتی[۷] (SAR)**

الزاماتی برای تضمین امنیت محصول.

۲-۲- اصطلاحات تکنولوژی

- **تصادفی‌سازی چیدمان فضای آدرس[۸] (ASLR)**

یک ویژگی ضد استخراج که نگاشت‌های حافظه را در مکان‌های غیرقابل پیش‌بینی بارگذاری می‌کند. تصادفی‌سازی چیدمان فضای آدرس، تغییر مسیر کنترل بر روی کدهایی که به فضای آدرس در یک فرایند معرفی شده‌اند را برای مهاجم دشوار می‌سازد.

- **مدیر سیستم[۹]**

مدیر سیستم مسئول اقدامات مدیریتی از جمله تنظیم خط‌مشی‌های به‌کار گرفته شده توسط شرکت بر روی سیستم‌عامل است. این مدیر سیستم می‌تواند از راه دور از طریق یک سرور مدیریتی و از جایی فعالیت کند که این سامانه خط‌مشی‌های پیکربندی را دریافت می‌کند. یک مدیر سیستم می‌تواند تنظیماتی بر روی سامانه اعمال کند که توسط کاربرانی غیر از مدیر سیستم قابل‌بازنویسی نباشد.

---

[۶] Security Functional Requirement

[۷] Security Assurance Requirement

[۸] Address Space Layout Randomization

[۹] Administrator

- **برنامه‌کاربردی**[۱۰] (app)

نرم‌افزاری که بر روی یک سکو اجرا می‌شود و وظایفی را از سوی کاربر یا صاحب سکو انجام می‌دهد، به علاوه مستندات پشتیبانی‌کننده آن.

- **رابط برنامه‌نویسی برنامه‌کاربردی**[۱۱] **(API)**

مشخصات روال‌ها، ساختارهای داده، کلاس‌های موجودیت‌های غیرفعال، و متغیرهایی که به برنامه‌کاربردی اجازه استفاده از خدمات ارائه‌شده توسط مؤلفه نرم‌افزاری دیگر مانند یک کتابخانه را می‌دهد. رابط‌های برنامه‌نویسی برنامه‌کاربردی اغلب برای مجموعه‌ای از کتابخانه‌های گنجانده شده در سکو ارائه شده‌اند.

- **اعتبارنامه**[۱۲]

داده‌هایی که هویت یک کاربر را به طور مثال یک کلید رمزنگاری یا کلمه‌عبور را تعیین می‌کنند.

- **پارامترهای امنیتی حیاتی**[۱۳] **(CSP)**

اطلاعات تعریف‌شده کاربر یا سامانه که برای اجرای یک پیمانه رمزنگاشتی در پردازش توابع رمزگذاری از جمله کلیدهای رمزنگاری و داده احراز هویت، مانند کلمه‌عبورها، مورد استفاده است و افشا یا تغییری در آن‌ها می‌تواند امنیت واحد رمزنگاشتی یا امنیت اطلاعات محافظت شده توسط واحد را به خطر بیندازد.

- **محافظت از داده‌های در حال سکون**[۱۴] **(DAR)**

---

[۱۰] Application

[۱۱] Application Programming Interface

[۱۲] Credential

[۱۳] Critical Security Parameters

[۱۴] Data At Rest (DAR) Protection

اقدامات مقابله‌ای که از استخراج داده از انبارش غیرفرّار توسط مهاجمان جلوگیری می‌کنند، حتی آن‌هایی که دسترسی فیزیکی دارند. تکنیک‌های رایج آن رمزگذاری داده و پاکسازی[۱۵] است.

- **ممانعت از اجرای داده[۱۶] (DEP)**

یک ویژگی ضد استخراج از سیستم‌عامل‌های پیشرفته که برروی سخت‌افزارهای کامپیوتری مدرنی اجرا می‌شود که مجوز غیراجرایی را روی صفحات حافظه اعمال می‌کنند. ممانعت از اجرای داده از گنجاندن داده‌ها و دستورالعمل‌ها بر روی صفحات حافظه جلوگیری می‌کند که معرفی و اجرای کدها را برای مهاجم دشوار می‌سازد.

- **توسعه‌دهنده[۱۷]**

موجودیتی که نرم‌افزار سیستم‌عامل را می‌نویسد. با توجه به مقاصد این سند، توسعه‌دهندگان و فروشندگان یکی هستند.

- **دیواره آتش مبتنی بر میزبان[۱۸]**

پیاده‌سازی دیواره آتش مبتنی بر نرم‌افزار در حال اجرا بر روی سیستم‌عامل برای پالایش ترافیک شبکه ورودی به و خروجی از فرایندهای در حال اجرا بر روی سیستم‌عامل.

- **سیستم‌عامل[۱۹] (OS)**

---

[۱۵] wiping

[۱۶] Data Execution Prevention (DEP)

[۱۷] Developer

[۱۸] Host-based Firewall

[۱۹] Operating System

نرم‌افزاری که منابع فیزیکی و منطقی را مدیریت می‌کند و خدماتی برای برنامه‌های کاربردی ارائه می‌دهد. در این سند اصطلاح محصول و سیستم‌عامل قابل معاوضه هستند.

- **اطلاعات قابل‌شناسایی شخصی[۲۰] (PII)**

هرگونه اطلاعات در مورد یک فرد که توسط یک کارگزار حفظ و نگه‌داری می‌شود، و می‌تواند شامل اطلاعات تحصیلی، تراکنش‌های مالی، سوابق پزشکی، و سابقه کیفری یا سابقه اشتغال وی و همچنین اطلاعاتی باشد که می‌تواند برای تمایز یا ردیابی هویت فردی استفاده شود مانند نام فرد، شماره بیمه تأمین اجتماعی، تاریخ و محل تولد، نام مادر، و سوابق بیومتریک و غیره، و همچنین شامل هرگونه اطلاعات شخصی‌ای که مرتبط و یا قابل ارتباط به یک فرد می‌باشد. [OMB]

- **داده حساس[۲۱]**

داده‌های حساس ممکن است شامل همه داده‌های کاربر یا شرکت شود و یا ممکن است داده برنامه‌کاربردی خاصی مانند اطلاعات قابل شناسایی شخصی، ایمیل‌ها، پیام‌ها، اسناد، اقلام تقویمی و اطلاعات تماس باشند. داده حساس باید حداقل شامل اعتبارنامه‌ها و کلیدها باشد. داده حساس باید در خلاصه مشخصه محصول (TSS) سیستم‌عامل توسط نویسنده هدف امنیتی مشخص شده باشد.

- **کاربر[۲۲]**

کاربر در خط‌مشی‌های پیکربندی به‌کار گرفته شده توسط مدیر سیستم برای سیستم‌عامل یک موجودیت فعال است. در برخی از سامانه‌ها تحت شرایط پیکربندی معینی، کاربر عادی می‌تواند به‌طور موقت امتیازاتش به اندازه یک مدیر سیستم بالا رود. در این زمان، چنین کاربری باید به عنوان مدیر سیستم در نظر گرفته شود.

---

[۲۰] Personally Identifiable Information

[۲۱] Sensitive Data

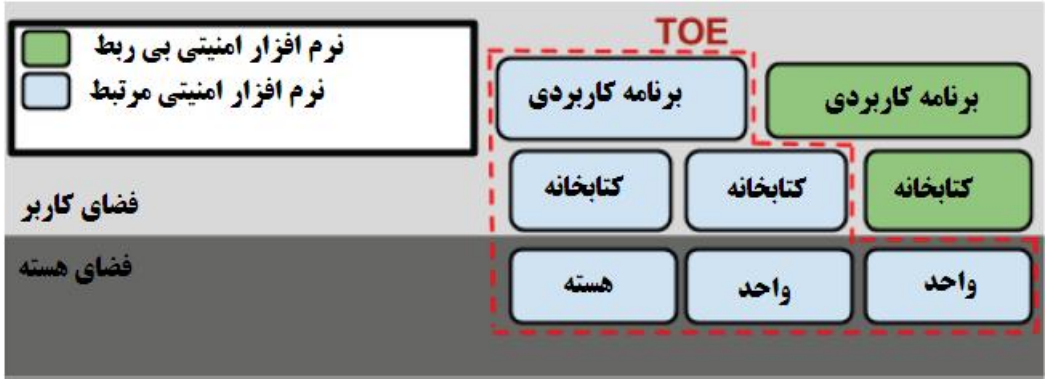
[۲۲] User

۳- شرح محصول

۳-۱- مرزهای محصول

مرز محصول شامل هسته سیستم‌عامل و درایورهای آن، کتابخانه‌های نرم‌افزار مشترک[۲۳]، و برخی از نرم‌افزارهای برنامه‌های کاربردی گنجانده شده در سیستم‌عامل می‌باشد. برنامه‌های کاربردی که در محصول مورد توجه قرار می‌گیرند آنهایی هستند که خدمات امنیتی اساسی را ارائه می‌دهند، بسیاری از آن‌ها با امتیازات افزایش‌یافته اجرا می‌شوند.

برنامه‌های کاربردی‌ای که توسط پروفایل‌های حفاظتی مشخص‌تری تحت پوشش قرار گرفته‌اند نمی‌توانند به عنوان بخشی از ارزیابی سیستم‌عامل مورد ادعای ارزیابی قرار گیرند، حتی زمانی که ارزیابی برخی از قابلیت‌های کارکردی آن‌ها که مرتبط با نقش آن‌ها به عنوان بخشی از سیستم‌عامل است ضروری باشد.



شکل ۱ محصول کلی

۳-۲- سکوی محصول

[۲۳] shared software libraries

سکوی محصول که متشکل از سخت‌افزارهای فیزیکی و یا مجازی است که محصول روی آن اجرا می‌شود، بیرون از دامنه ارزیابی است. با این حال امنیت محصول به آن وابسته است. دیگر مؤلفه‌های سخت‌افزاری‌ای که به طور مستقل نرم‌افزارهای خود را اجرا می‌کنند و مرتبط با امنیت کلی سامانه می‌باشد نیز خارج از دامنه ارزیابی هستند.

۳-۳-حالت‌های استفاده

الزامات موجود در این پروفایل حفاظتی برای رسیدگی به مسائل امنیت در حداقل حالت‌های استفاده زیر طراحی شده‌اند. این حالت‌های استفاده به طور عمدی گسترده در نظر گرفته شده است به طوریکه حالت‌های استفاده مشخص برای یک سیستم‌عامل وجود دارد. این حالت‌های استفاده ممکن است با دیگری همپوشانی داشته باشد.

قابلیت کارکردی یک سیستم‌عامل حتی ممکن است به طور مؤثر توسط برنامه‌های کاربردی امتیاز داده شده نصب شده بر روی آن توسعه یابد.

در هر صورت این موارد خارج از هدف و دامنه کاربرد این پروفایل حفاظتی هستند.

۳-۳-۱- [حالت استفاده ۱] افزاره‌های کاربر نهایی

سیستم‌عامل سکوی برای افزاره‌های کاربر نهایی مانند کامپیوترهای رومیزی، لپ‌تاپ‌ها، تبدیل‌پذیرها و تبلت‌ها فراهم می‌آورد. این افزاره‌ها ممکن است به صورت اختیاری دامنه کاربرد یک سرور دایرکتوری و یا یک سرور مدیریتی باشند.

از آنجا که این پروفایل حفاظتی تهدیدات متوجه داده‌های در حال سکون را مورد توجه قرار نمی‌دهد، شرکت‌هایی که سیستم‌عامل‌هایی را در سناریوهای سیّار توسعه می‌دهند باید اطمینان حاصل نمایند که این سامانه‌ها حفاظت از داده‌های در حال سکون نوشته شده در دیگر پروفایل‌های حفاظتی را شامل شود. به‌ویژه، این شامل *پروفایل‌های حفاظتی برای رمزگذاری درایو کامل – موتور رمزگذاری، رمزگذاری درایو کامل – اکتساب مجوز، و رمزگذاری فایل نرم‌افزار* می‌باشد. *پروفایل حفاظتی برای شالوده افزاره‌های سیّار* شامل الزاماتی برای حفاظت از داده‌های در حال سکون می‌باشد و برای بسیاری از افزاره‌های سیّار مناسب است.

۳-۳-۲- [حالت استفاده ۲] سامانه‌های سرور

سیستم‌عامل سکوی برای خدمات سمت سرور بر روی سخت‌افزارهای فیزیکی یا مجازی فراهم می‌آورد. مثال‌های مشخصی وجود دارد که سیستم‌عامل به عنوان سکوی برای چنین خدماتی عمل می‌نماید مانند سرورهای فایل، سرورهای پستی، و سرورهای وب.

۳-۳-۳- [حالت استفاده ۳] سامانه‌های ابری

سیستم‌عامل سکوی برای ارائه خدمات ابری در حال اجرا بر روی سخت‌افزارهای فیزیکی یا مجازی فراهم می‌آورد. سیستم‌عامل معمولاً قسمتی از ارائه‌های شناسایی شده به عنوان زیرساخت به عنوان یک خدمت (IaaS[۲۴])، نرم‌افزار به عنوان یک خدمت (SaaS[۲۵])، و سکو به عنوان یک خدمت (PaaS[۲۶]) می‌باشد.

این حالت استفاده معمولاً استفاده از تکنولوژی مجازی‌سازی را نیز در بر می‌گیردکه توصیه می‌شود بر اساس *پروفایل حفاظتی مجازی‌سازی سرور* ارزیابی شود.

۴-مسائل امنیتی

۴-۱- کلیات

مسئله امنیتی بر اساس تهدیداتی که انتظار می‌رود سیستم‌عامل مورد توجه قرار دهد، مفروضاتی درباره محیط عملیاتی، و هر خط‌مشی امنیت سازمانی که سیستم‌عامل انتظار می‌رود اجرا کند، توصیف می‌شود.

۴-۲- تهدیدات

[۲۴] Infrastructure as a Service

[۲۵] Software as a Service

[۲۶] Platform as a Service

تهدیدات	توضیحات
T.NETWORK_ATTACK	مهاجم در کانال ارتباطاتی یا هر جای دیگر در زیرساخت شبکه جایگیری کرده است. مهاجمان ممکن است در ارتباطات با برنامه‌های کاربردی و خدمات در حال اجرا بر روی قسمتی از سیستم‌عامل با نیت ایجاد خطر شرکت کنند. این مشارکت ممکن است شامل تغییر ارتباطات قانونی موجود باشد.
T.NETWORK_EAVESDROP	مهاجم که در کانال ارتباطی یا هر جای دیگری در زیرساخت شبکه جایگیری کرده است. مهاجمان ممکن است بر داده‌های رد و بدل شده بین برنامه‌های کاربردی و خدماتی که بر روی قسمتی از سیستم‌عامل در حال اجرا هستند نظارت و دسترسی داشته باشند.
T.LOCAL_ATTACK	مهاجمی که ممکن است برنامه‌های کاربردی در حال اجرا بر روی سیستم‌عامل را به خطر بیندازد. برنامه‌های کاربردی به‌خطر افتاده ممکن است ورودی قالب داده شده مخربی را از طریق کانال‌های گوناگونی از جمله فراخوانی سامانه‌های غیرمجاز و پیام‌رسانی از طریق سامانه فایل به سیستم‌عامل ارائه دهد.
T.LIMITED_PHYSICAL_ACCESS	مهاجم ممکن است در حالی‌که زمان محدودی دارد تلاش کند تا با افزاره فیزیکی به داده‌های موجود بر روی سیستم‌عامل دسترسی پیدا کند.

۴-۳- مفروضات

مفروضات	توضیحات
A.PLATFORM	سیستم‌عامل برای اجرا متکی به سکوی محاسباتی قابل‌اعتمادی است. این سکوی زیرین، خارج از هدف و دامنه کاربرد این پروفایل حفاظتی است.
A.PROPER_USER	کاربر سیستم‌عامل عمداً غفلت نکرده و یا خصومتی ندارد و از نرم‌افزار مطابق با خط‌مشی‌های امنیتی به‌کار گرفته شده در خط‌مشی امنیتی شرکت استفاده می‌کند. با این حال، نرم‌افزارهای مخرب می‌توانند به عنوان کاربر عمل کنند، بنابراین الزاماتی که موجودیت‌های فعال مخرب را محدود می‌کند هنوز در دامنه کاربرد این پروفایل حفاظتی است.
A.PROPER_ADMIN	مدیر سیستم سیستم‌عامل بی دقت نیست و یا عمداً غفلت نکرده و خصومتی ندارد و سیستم‌عامل را مطابق با خط‌مشی امنیتی به‌کار گرفته در خط‌مشی امنیتی شرکت اجرا و اداره کند.

۵- اهداف امنیتی

۵-۱- کلیات

این بخش به شناخت و معرفی اهداف امنیتی هدف ارزیابی و محیط آن می‌پردازد. اهداف امنیتی منعکس کننده مقاصد مشخص و مقابله با تهدیدهای شناخته شده و مطابق با مفروضات و سیاست‌های امنیتی تعیین شده است.

۵-۲- اهداف امنیتی برای محصول

هدف امنیتی محصول	توضیحات
O.ACCOUNTABILITY	سیستم‌عامل‌های منطبق بر این پروفایل حفاظتی، اطمینان حاصل می‌کنند که اطلاعاتی وجود دارد که به مدیران سیستم اجازه می‌دهد موضوعات غیرعمدی موجود در مورد پیکربندی و عملکرد سیستم‌عامل و دلایل ایجاد آن‌ها را کشف کنند. جمع‌آوری اطلاعات رویداد و انتقال فوری آن به سامانه‌های دیگر می‌تواند پاسخ به رویدادهایی که سامانه را به خطر انداخته‌اند را میسر کند. این موضوع در الزام کارکرد امنیتی تولید داده ممیزی[۲۷] مورد توجه قرار گرفته است.
O.INTEGRITY	سیستم‌عامل‌های منطبق بر این پروفایل حفاظتی، از یکپارچگی بسته‌های به‌روزرسانی خود اطمینان حاصل می‌کنند. سیستم‌عامل‌ها اگر نگوییم هرگز ولی به‌ندرت بدون خطا فرستاده می‌شوند در نتیجه توانایی استقرار تکه‌ها[۲۸] و به‌روزرسانی یکپارچه و منسجم سیستم برای امنیت شبکه شرکت بسیار مهم و حیاتی است. سیستم‌عامل‌های منطبق بر این پروفایل حفاظتی، اجرای عوامل کاهش خطر مبتنی بر محیط را فراهم می‌آورند که با افزودن پیچیدگی به وظایف سامانه‌های در معرض خطر، هزینه را برای مهاجمان افزایش می‌دهد. این موضوع مورد توجه الزامات کارکرد امنیتی زیر قرار دارد: FPT_SBOP_EXT.1, FPT_ASLR_EXT.1, FPT_TUD_EXT.1, FPT_TUD_EXT.2, FCS_COP.1.1(2), FCS_COP.1.1(3), FCS_COP.1.1(4), FPT_ACF_EXT.1, FPT_SRP_EXT.1, FIA_X509_EXT.2, FPT_TST_EXT.1, FTP_ITC_EXT.1, FPT_W^X_EXT.1.1, FIA_AFL.1, FIA_UAU.5

[۲۷] FAU_GEN.1

[۲۸] patches

O.MANAGEMENT	به‌منظور تسهیل مدیریت توسط کاربر و شرکت، سیستم‌عامل‌های منطبق بر این پروفایل حفاظتی، رابط‌های سازگار و پشتیبانی شده‌ای برای پیکربندی و نگهداشت‌های مرتبط با امنیت آن‌ها فراهم می‌آورند. این رابط‌ها شامل گسترش برنامه‌های کاربردی و به‌روز رسانی‌های برنامه‌کاربردی با استفاده از ساز و کارها و قالب‌های گسترش پشتیبانی شده توسط سکو و همچنین ارائه ساز و کارهایی برای پیکربندی و کنترل اجرای برنامه‌کاربردی می‌باشد. این موضوع مورد توجه الزامات کارکرد امنیتی زیر قرار دارد: FMT_MOF_EXT.1, FTP_TRP.1
O.PROTECTED_STORAGE	سیستم‌عامل‌های منطبق بر این پروفایل حفاظتی برای رسیدگی به موضوع فقدان محرمانگی اعتبارنامه‌ها در رویداد از دست دادن کنترل فیزیکی رسانه انبارش، حفاظت از داده‌های در حال سکون را برای اعتبارنامه‌ها فراهم می‌آورند. همچنین این سیستم‌عامل‌ها کنترل دسترسی ارائه می‌دهند که به یک کاربر اجازه محافظت از فایل‌های خصوصی از دسترس دیگر کاربران همان سامانه را می‌دهد. این موضوع مورد توجه الزامات کارکرد امنیتی زیر قرار دارد: FCS_STO_EXT.1, FCS_RBG_EXT.1, FCS_COP.1.1 (1), FDP_ACF_EXT.1.
O.PROTECTED_COMMS	سیستم‌عامل‌های منطبق بر این پروفایل حفاظتی برای رسیدگی به تهدیدات حمله به شبکه انفعالی (استراق سمع) و فعال (تغییر بسته)، ساز و کارهایی برای ایجاد کانال‌های قابل‌اعتماد برای پارامترهای امنیتی حیاتی و داده‌های حساس فراهم می‌آورند. هم پارامترهای امنیتی حیاتی و هم داده‌های حساس نمی‌توانند خارج از سکو اجرا شوند. این موضوع مورد توجه الزامات کارکرد امنیتی زیر قرار دارد: FCS_TLSC_EXT.1, FCS_TLSC_EXT.2, FCS_TLSC_EXT.3, FCS_TLSC_EXT.4, FCS_DTLS_EXT.1, FCS_RBG_EXT.1, FCS_CKM.1, FCS_CKM.2, FCS_COP.1.1(1), FDP_IFC_EXT.1, FIA_X509_EXT.1, FIA_X509_EXT.2, FTP_ITC_EXT.1.

۵-۳-اهداف امنیتی برای محیط عملیاتی

اهداف امنیتی زیر برای محیط عملیاتی به سیستم‌عامل در فراهم آوردن درست قابلیت‌های کارکرد امنیتی خود کمک می‌کند. این اهداف مفروضات درباره محیط را پیگیری خواهد نمود.

هدف امنیتی محیط عملیاتی	توضیحات
OE.PLATFORM	سیستم‌عامل متکی بر این است که بر روی سخت‌افزار قابل‌اعتمادی نصب شده باشد.
OE.PROPER_USER	کاربر سیستم‌عامل عمداً غفلت نمی‌کند و یا خصومتی ندارد، و از نرم‌افزار مطابق خط‌مشی امنیتی به کار گرفته شده توسط شرکت استفاده می‌کند. حساب‌های کاربری استاندارد مطابق با مدل امتیازات حداقلی تهیه شده‌اند. کاربرانی که نیازمند سطوح بالاتر دسترسی هستند باید حساب جداگانه‌ای اختصاص‌یافته‌ای برای آن استفاده داشته باشند.
OE.PROPER_ADMIN	مدیر سیستم سیستم‌عامل بی‌دقت نیست و عمداً غفلت نمی‌کند و یا خصومتی ندارد، و سیستم‌عامل را مطابق خط‌مشی‌های به کار گرفته شده در شرکت اجرا و اداره می‌کند.

۵-۴- منطق اهداف امنیتی

این بخش توضیح می‌دهد که چگونه مفروضات، تهدیدات، و خط‌مشی‌های امنیتی سازمانی[۲۹] برای اهداف امنیتی ترسیم شده‌اند.

جدول ۱ توجیه مفروضات، تهدیدات و خط‌مشی‌های امنیت سازمانی ترسیم شده برای اهداف امنیتی

تهدید، مفروضات و یا خط‌مشی امنیتی سازمانی	اهداف امنیتی	توجیه
تهدید حمله شبکه (T.NETWORK_ATTACK)	هدف امنیتی ارتباطات حفاظت‌شده (O.PROTECTED_COMMS)، هدف امنیتی یکپارچگی (O.INTEGRITY)، هدف امنیتی مدیریت (O.MANAGEMENT).	هنگامی که هدف امنیتی ارتباطات حفاظت‌شده، یکپارچگی داده‌ی انتقال یافته را تامین می‌کند با تهدید حمله شبکه مقابله می‌شود.
		هنگامی که هدف امنیتی یکپارچگی، یکپارچگی نرم‌افزار نصب شده بر روی سامانه شبکه را تامین می‌کند با تهدید حمله شبکه مقابله می‌کند.
		هنگامی که هدف امنیتی مدیریت، توانایی پیکربندی سیستم‌عامل برای دفاع در مقابل تهدید شبکه را فراهم می‌کند با تهدید حمله شبکه مقابله می‌کند.

[۲۹] Organizational Security Policy (OSP)

تهدید استراق سمع شبکه (T.NETWORK_EAVESDROP)	هدف امنیتی ارتباطات حفاظت‌شده (O.PROTECTED_COMMS)، هدف امنیتی مدیریت (O.MANAGEMENT)	هنگامی که هدف امنیتی ارتباطات حفاظت‌شده، محرمانگی داده‌های انتقال‌یافته را تامین می‌کند، با تهدید استراق سمع شبکه مقابله می‌کند.
		هنگامی که هدف امنیتی مدیریت، توانایی پیکربندی سیستم‌عامل را جهت محافظت از محرمانگی داده‌های انتقال‌یافته‌اش فراهم می‌آورد، با تهدید استراق سمع شبکه مقابله می‌کند.
تهدید حمله محلی (T.LOCAL_ATTACK)	هدف امنیتی یکپارچگی (O.INTEGRITY)	هنگامی که هدف امنیتی یکپارچگی، در مقابل استفاده از ساز و کارهایی که محصول را با توجه حملات دیگر نرم‌افزارهای موجود بر سکو تضعیف می‌کند، محافظت می‌کند.
تهدید دسترسی فیزیکی محدود (T.LIMITED_PHYSICAL_ACCESS)	هدف امنیتی انبارش حفاظت‌شده (O.PROTECTED_STORAGE)	هدف امنیتی انبارش حفاظت‌شده در مقابل تلاش‌های غیرمجاز برای دسترسی به انبارش فیزیکی استفاده‌شده توسط محصول محافظت می‌کند.

فرض سکو (A.PLATFORM)	هدف امنیتی سکو (OE.PLATFORM)	هدف امنیتی محیط عملیاتی سکو با فرض سکو تحقق می‌یابد.
فرض کاربر شایسته (A.PROPER_USER)	هدف امنیتی کاربر شایسته (OE.PROPER_USER)	هدف امنیتی محیط عملیاتی کاربر شایسته با فرض کاربر شایسته تحقق می‌یابد.
فرض مدیر سیستم شایسته (A.PROPER_ADMIN)	هدف امنیتی مدیر سیستم شایسته (OE.PROPER_ADMIN)	هدف امنیتی محیط عملیاتی مدیر سیستم شایسته با فرض مدیر سیستم شایسته تحقق می‌یابد.

۶-الزامات کارکرد امنیتی

۶-۱- قراردادها

الزامات کارکرد امنیتی موجود در این بخش از قسمت ۲ معیار مشترک برای ارزیابی امنیت فناوری اطلاعات، نسخه ۳,۱، بازبینی ۴، همراه با مؤلفه‌های کارکردی توسعه داده شده افزوده استخراج شده است. نشانه‌گذاری‌های زیر مورد استفاده خواهند بود:

- عملیات **پالایش** (:با **متن پر رنگ** مشخص شده است): برای افزودن جزئیات به یک الزام و بنابراین محدود کردن بیشتر یک الزام مورد استفاده قرار می‌گیرد.
- **انتخاب** (با *نوشته‌های مورب* مشخص می‌شود): برای انتخاب یک و یا چند گزینه ارائه شده توسط معیار مشترک در بیان یک الزام مورد استفاده قرار می‌گیرد.
- عملیات **اختصاص** (با *نوشته‌های مورب* مشخص می‌شود): برای اختصاص یک مقدار مشخص به یک پارامتر نامشخص مانند طول یک کلمه‌عبور مورد استفاده قرار می‌گیرد. اختصاص با نشان دادن مقادیر در براکت نشان داده می‌شود.

- عملیات **تغییر**: با یک عدد درون پرانتز مشخص می‌شود (به عنوان مثال ("(۱)").

الزامات کارکرد امنیتی برای سیستم‌عامل همه‌منظوره، با توجه به الزاماتی که در استاندارد ارزیابی معیار مشترک مطرح گردیده، به صورت خلاصه در Error! Reference source not found.زیر آورده شده است.

جدول ۲ الزامات کارکرد امنیتی

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱	**تولید کلید رمزنگاری ۱**	FCS_CKM.1
۲		
۳	**برقراری کلید رمزنگاری**	FCS_CKM.2
۴	**تخریب کلید رمزنگاری توسعه‌یافته**	FCS_CKM_EXT.3
۵	**عملیات رمزنگاری - رمزگذاری/رمزگشایی**	FCS_COP.1(1)
۶	**عملیات رمزنگاری – چکیده‌سازی**	FCS_COP.1(2)
۷	**عملیات رمزنگاری – امضا کردن**	FCS_COP.1(3)
۸	**عملیات رمزنگاری – احراز هویت پیام چکیده کلیددار**	FCS_COP.1(4)
۹	**تولید بیت تصادفی**	FCS_RBG_EXT.1
۱۰	**انبارش داده حساس**	FCS_STO_EXT.1
۱۱	**پروتکل TLS سرویس‌گیرنده (کلاینت)**	FCS_TLSC_EXT.1
۱۲	**مشخصه‌های امنیتی مبتنی بر کنترل دسترسی برای حفاظت از داده کاربر**	FDP_ACF_EXT.1
۱۳	**خط‌مشی کنترل جریان اطلاعات**	FDP_IFC_EXT.1
۱۴	**مدیریت رفتار توابع امنیتی**	FMT_MOF_EXT.1

شماره الزام	نام الزام	تطابق الزام با استاندارد
۱۵	کنترل‌های دسترسی	FPT_ACF_EXT.1
۱۶	تصادفی‌سازی چیدمان فضای آدرس	FPT_ASLR_EXT.1
۱۷	حفاظت از سرریز بافر پشته	FPT_SBOP_EXT.1
۱۸	یکپارچگی راه‌اندازی	FPT_TST_EXT.1
۱۹	یکپارچگی نصب و به‌روزرسانی	FPT_TUD_EXT.1
۲۰	یکپارچگی نصب و به‌روزرسانی نرم‌افزار برنامه‌کاربردی	FPT_TUD_EXT.2
۲۱	تولید داده ممیزی امنیتی	FAU_GEN.1
۲۲	ساماندهی شکست در احراز هویت	FIA_AFL.1
۲۳	ساز و کارهای احراز هویت چندگانه	FIA_UAU.5
۲۴	اعتبارسنجی گواهی X.509	FIA_X509_EXT.1
۲۵	اعتبارسنجی گواهی X.509	FIA_X509_EXT.2
۲۶	ارتباط کانال قابل‌اعتماد	FTP_ITC_EXT.1
۲۷	مسیر قابل‌اعتماد	FTP_TRP.1

۶-۲- کلاس پشتیبانی رمزنگاری

شماره الزام	نام الزام
۱	**تولید کلید رمزنگاری ۱**

سیستم‌عامل باید کلیدهای رمزنگاری نامتقارنی مطابق با الگوریتم تولید کلید رمزنگاری مشخص‌شده [**انتخاب**:

طرح‌های RSA [۳۰] *با استفاده از اندازه‌های کلید رمزنگاری ۲۰۴۸ بیت یا بیشتر، که: [انتخاب: استاندارد انتشارات استانداردهای پردازش اطلاعات فدرال ۴-۱۸۶* [۳۱]*، "امضای دیجیتال استاندارد (DSS)"، پیوست. B.3، ANSI X9.311998، بخش ۴,۱] را برآورده می‌سازد،*

طرح‌های ECC[۳۲] *با استفاده از "خم‌های NIST* [۳۳] *"P-256، P-384 و [انتخاب: P-521، هیچ خم دیگری] که: [انتخاب: انتشارات استانداردهای پردازش اطلاعات فدرال سال ۴-۱۸۶، "امضای دیجیتال استاندارد (DSS)"، پیوست. B.4] را برآورده می‌سازد*] تولید کند.

نکته کاربردی ۱: نویسنده هدف امنیتی باید همه طرح‌های تولید کلید مورد استفاده برای برقراری کلید و احراز هویت موجودیت را انتخاب کند. هنگامی که تولید کلید برای برقراری کلید مورد استفاده قرار گرفت، طرح‌های موجود در عنصر ۱ برقراری کلید رمزنگاری (FCS_CKM.2.1) و پروتکل‌های رمزنگاری انتخاب شده با انتخاب تطبیق داشته باشند. زمانی که تولید کلید برای احراز هویت موجودیت استفاده شد، انتظار می‌رود کلید عمومی با یک گواهی X.509v3 مرتبط باشد.

---

[۳۰] RSA از ابتدای نام خانوادگی ران رایوست (Ron Rivest)، ادی شامیر (Adi Shami) و لئونارد ادلمن (Leonard Adleman) تشکیل شده که اولین بار در سال ۱۹۷۷ الگویتم را به صورت عمومی توضیح دادند.

[۳۱] **FIPS PUB 186-4**: Federal Information Processing Standards Publications

[۳۲] Elliptic curve cryptography (ECC):

رویکردی است برای رمزنگاری کلید عمومی مبتنی بر ساختار جبری خم‌های بیضوی بر روی رشته‌های نامتناهی. یکی از مزایای اصلی در مقایسه با رمزنگاری غیر منحنی بیضوی (با رشته‌های گلوای مسطح به عنوان مبنا) سطح امنیت ارائه شده یکسان با کلیدهای کوچکتر از نظر اندازه می‌باشد.

[۳۳] U.S. National Institute of Standards and Technology

چنانچه سیستم‌عامل در طرح برقراری کلید RSA تنها به عنوان دریافت‌کننده عمل کند، نیازی نیست سیستم‌عامل تولید کلید RSA را پیاده‌سازی کند. گزینه انتخابی ANSI X9.311998 در انتشارات آینده این سند از انتخاب حذف خواهد شد. در حال حاضر برای اینکه به صنعت زمان بیشتری داده شود تا انتقال به استاندارد FIPS PUB 186-4 پیشرفته را تکمیل کند، این انتخاب تنها محدود به گزینه‌های انتخابی FIPS PUB 186-4 نیست.
۲ **برقراری کلید رمزنگاری ۱**
سیستم‌عامل باید قابلیت‌های کارکردی‌ای برای انجام برقراری کلید رمزنگاری مطابق با روش برقراری کلید رمزنگاری مشخص پیاده‌سازی کند: **طرح‌های برقراری کلید مبتنی بر RSA** که موارد زیر را برآورده می‌سازد: استاندارد انتشارات ویژه مؤسسه ملی استاندارد 800-56B، "توصیه‌هایی برای طرح‌های برقراری کلید دو به دو با استفاده از رمزنگاری فاکتورگیری عدد صحیح" و [**انتخاب**: ***طرح‌های برقراری کلید مبتنی بر منحنی بیضوی*** *که مورد زیر را برآورده می‌سازد: استانداردهای انتشارات ویژه مؤسسه ملی استاندارد 800-56B "، توصیه‌هایی برای طرح‌های برقراری کلید دو به دو با استفاده از رمزنگاری لگاریتم گسسته*[۳۴]"، *هیچ طرح دیگری*]. **نکته کاربردی ۲:** نویسنده هدف امنیتی باید همه طرح‌های برقراری کلید مورد استفاده برای پروتکل‌های رمزنگاری منتخب را انتخاب کند. الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS (FCS_TLSC_EXT.1) به دنباله‌های رمزی نیاز دارد که از طرح‌های برقراری کلید مبتنی بر RSA استفاده می‌کنند. طرح‌های برقراری کلید مبتنی بر RSA در بخش ۹ استاندارد NIST SP 800-56B توضیح داده شده‌اند؛ با این حال، بخش ۹ متکی بر پیاده‌سازی بخش‌های دیگر استاندارد NIST SP 800-56B می‌باشد. اگر سیستم‌عامل در طرح برقراری کلید مبتنی بر RSA به عنوان دریافت‌کننده عمل کند، نیازی به پیاده‌سازی تولید کلید RSA نخواهد داشت. خم‌های بیضوی مورد استفاده برای طرح برقراری باید با خم‌های مشخص شده در عنصر ۱ الزام کارکرد امنیتی تولید کلید رمزنگاری (FCS_CKM.1.1) همبستگی داشته باشند.

[۳۴] Discrete Logarithm Cryptography

۳	تخریب کلید رمزنگاری توسعه‌یافته ۱
سیستم‌عامل باید کلیدهای رمزنگاری را طبق روش‌های تخریب کلید رمزنگاری مشخص‌شده از بین ببرد. [**انتخاب**: برای حافظه فرّار، تخریب باید با بازنویسی مستقیم منحصر به‌فرد [انتخاب: متشکل از یک الگوی شبه‌تصادفی با استفاده از تولیدکننده بیت تصادفی توابع هدف امنیتی، متشکل از صفرها] انجام شود که از یک الگوی بررسی - خواندن استنباط شده است. چنانچه درستی‌سنجی - خواندن داده بازنویسی‌شده با شکست روبرو شود، فرایند باید مجدداً تکرار شود. برای حافظه غیرفرّار فقط خواندنی قابل برنامه‌ریزی و پاک کردن به وسیله سیگنال‌های الکتریکی (EEPROM)[۳۵]، تخریب باید با بازنویسی مستقیم منحصر به‌فرد متشکل از الگوی شبه‌تصادفی با استفاده از تولید بیت تصادفی توابع هدف امنیتی (به‌گونه‌ای که در الزام کارکرد امنیتی تولید بیت تصادفی توسعه‌یافته (FCS_RBG_EXT.1) مشخص شده است) انجام شود که از یک الگوی بررسی – خواندن تبعیت شده‌است. چنانچه درستی‌سنجی - خواندن داده بازنویسی شده با شکست روبرو شود، فرایند باید مجدداً تکرار شود. برای حافظه‌های فلش غیر فرّار، تخریب باید با [**انتخاب**: بازنویسی مستقیم منحصر به‌فرد متشکل از صفر، پاک کردن قالب] تبعیت‌شده از یک الگوی بررسی - خواندن اجرا شود. چنانچه درستی‌سنجی - خواندن داده‌های بازنویسی شده با شکست روبرو شود، فرایند باید مجدداً تکرار شود. برای حافظه غیرفرّار دیگری به جز EEPROM و فلش، تخریب باید با بازنویسی سه بار یا بیشتر الگوی تصادفی‌ای که قبل از هر نوشتن تغییر کرده است اجرا شود]. **نکته کاربردی ۳:** پاکسازی نشان داده‌شده در بالا برای هر ناحیه انبارش میانجی که در انتقال کلید به مکان دیگر وجود دارد به‌کار می‌رود.	
۴	**عملیات رمزنگاری – رمزگذاری / رمزگشایی ۱**
سیستم‌عامل باید خدمات رمزگذاری / رمزگشایی داده را مطابق یک الگوریتم رمزنگاری مشخص انجام دهد. • مد AES-XTS (همانگونه که در NIST SP 800-38E تعریف شده است)؛ • مد AES-CBC (همانگونه که در NIST SP 800-38A تعریف شده است)؛ • مد AES-CCMP (همانگونه که در FIPS PUB 197، NIST SP 800-38C و IEEE 802.11-2012 تعریف شده است)؛	

[۳۵] Electrically Erasable Programmable Read Only Memory

و [**انتخاب**: *پوشاندن کلید (KW[۳۶]) استاندارد رمزگذاری پیشرفته (AES[۳۷]) (همانگونه که در NIST SP 800-38F تعریف شده است)،* *پوشاندن کلید با لایه‌گذاری استاندارد رمزگذاری پیشرفته (KWP[۳۸]) (همانگونه که در NIST SP 800-38F تعریف شده است)،* *AES-GCM (همانگونه که در NIST SP 800-38D تعریف شده است)،* *AES-CCM (همانگونه که در NIST SP 800-38C تعریف شده است)،* *AES-CCMP-256 (همانگونه که در NIST SP 800-38C و IEEE 802.11-2012 تعریف شده است)،* *AES-GCMP-256 (همانگونه که در NIST SP 800-38D و IEEE 802.11ac-2013 تعریف شده است)،* مد دیگری *وجود ندارد*] و اندازه‌های کلید رمزنگاری ۱۲۸ بیت و ۲۵۶ بیتی. **نکته کاربردی ۴:** برای انتخاب اول، نویسنده هدف امنیتی بهتر است مد یا مدهایی را انتخاب نماید که در استاندارد رمزگذاری پیشرفته عمل می‌کند. برای انتخاب دوم، نویسنده هدف امنیتی بهتر است اندازه‌های کلیدهایی را انتخاب نماید که با این قابلیت کارکردی پشتیبانی شده‌اند. اگر اندازه کلید ۱۲۸ بیتی انتخاب شوند، لازم است با الزامات کارکرد امنیتی پروتکل سرویس‌گیرنده TLS (FCS_TLSC_EXT.1) و تولید کلید رمزنگاری (FCS_CKM.1) مطابقت داشته باشند.
۵ **عملیات رمزنگاری – چکیده‌سازی ۱**
سیستم‌عامل باید خدمات چکیده‌سازی رمزنگاری را مطابق با الگوریتم رمزنگاری مشخص SHA-1[۳۹] و مورد زیر انجام دهد. [**انتخاب**: *SHA-256*،

[۳۶] Key Wrap

[۳۷] Advanced Encryption Standard

[۳۸] Key Wrap with Padding

[۳۹] Secure Hash Algorithm:الگوریتم چکیده‌ساز امن

SHA-384، *SHA-512*، *الگوریتم‌های دیگری وجود ندارد.*] و اندازه‌های چکیده‌پیام ۱۶۰ و [**انتخاب**:*۲۵۶،۳۸۴،۵۱۲،اندازه‌های چکیده پیام دیگری وجود ندارد*] بیت که مورد زیر را برآورده می‌سازد: FIPS Pub 180-4 **نکته کاربردی ۵:** بر طبق اســتاندارد NIST SP 800-131A، SHA-1 دیگر اجازه تولید امضــاهای دیجیتال را ندارد، و SHA-1 برای درستی‌سنجی امضاهای دیجیتال شدیداً غیرقابل‌اعتماد است به‌طوری که ممکن است در پذیرفتن این امضاها مخاطره‌ای وجود داشته باشد. در حال حاضر به منظور انطباق با الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS (FCS_TLSC_EXT.1) و بسته به انتخاب الزام کارکرد امنیتی پیاده‌سازی DTLS (FCS_DTLS_EXT.1)، به SHA-1 نیاز است. فروشندگان به‌شدت تشویق شده‌اند تا به‌روز رسانی‌ای در پروتکل‌های خود انجام دهند که از خانواده SHA-2 پشتیبانی می‌کند، تا زمانی که پروتکل‌های به‌روز شده پشتیبانی می‌شوند، این پروفایل حفاظتی اجازه پشتیبانی از پیاده‌سازی‌های SHA-1 را مطابق SP 800-131A می‌دهد. هدف از این الزام مشخص کردن تابع چکیده‌ساز می‌باشد. انتخاب چکیده‌ساز باید انتخاب اندازه چکیده پیام را پشتیبانی کند. انتخاب چکیده‌ساز بهتر است با استحکام کلی الگوریتم مورد استفاده سازگار باشد.
۶ عملیات رمزنگاری – امضا کردن ۱
سیستم‌عامل باید خدمات امضای رمزنگاری (تولید و درستی‌سنجی) را مطابق با یک الگوریتم رمزنگاری مشخص انجام دهد. [**انتخاب**: ***طرح‌های RSA*** *با استفاده از اندازه کلیدهای ۲۰۴۸ بیتی یا بیشتر که مورد زیر را برآورده می‌کنند: FIPS PUB 186-4، بخش ۴، "استاندارد امضای دیجیتال (DSS)"،*

طرح‌های ECDSA *با استفاده از "خم‌های NIST" P-256، P-384 و [انتخاب: P-521، هیچ خم دیگری] که مورد زیر را برآورده می‌سازد: FIPS PUB 186-4، بخش ۵، "استاندارد امضای دیجیتال (DSS)"].* **نکته کاربردی ۶:** در صورتی که بیش از یک الگوریتم وجود داشته باشد نویسنده هدف امنیتی باید الگوریتم پیاده‌سازی شده‌ای برای انجام امضاهای دیجیتال را انتخاب کند، این الزام بایستی برای مشخص کردن قابلیت کارکردی تکرار شود. توصیه می‌شود نویسنده هدف امنیتی برای الگوریتم انتخاب شده انتخاب‌ها یا اختصاص‌های مناسب را ایجاد کند تا پارامترهایی که برای آن الگوریتم پیاده‌سازی شده‌اند را مشخص کند. تولید و درستی‌سنجی امضای RSA در حال حاضر مستلزم انطباق با الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS (FCS_TLSC_EXT.1) است.
۷ عملیات رمزنگاری – احراز هویت پیام چکیده کلید دار[۴۰] ۱
سیستم‌عامل باید خدمات احراز هویت پیام چکیده کلیددار را مطابق با الگوریتم رمزنگاری مشخص و مورد زیر انجام دهد. **[انتخاب**: *SHA-1،* *SHA-256،* *SHA-384،* *SHA-512،* *الگوریتم‌های دیگری وجود ندارد.*

[۴۰] Keyed-Hash Message

] و اندازه‌های کلید [**اختصاص**: اندازه کلید (بر حسب بیت) استفاده شده در کد احراز هویت پیام مبتنی بر چکیده‌پیام[۴۱] (HMAC)] و اندازه‌های چکیده پیام [**انتخاب**: *۱۶۰، ۲۵۶، ۳۸۴، ۵۱۲، هیچ اندازه دیگری*] بیتی که مورد زیر را برآورده می‌سازد: *کد احراز هویت پیام چکیده کلید دار* FIPS Pub 198-4 و *استاندارد چکیده‌ساز امن* FIPS Pub 180-4. **نکته کاربردی ۷:** هدف از این الزام مشخص کردن تابع احراز هویت پیام چکیده کلید دار مورد استفاده برای اهداف برقراری کلید برای پروتکل‌های رمزنگاری مختلفی است که توسط سیستم‌عامل استفاده شده است (به‌عنوان مثال کانال قابل اعتماد). انتخاب چکیده‌ساز باید انتخاب اندازه چکیده پیام را پشتیبانی کند. انتخاب چکیده‌ساز بهتر است با استحکام کلی الگوریتم مورد استفاده برای الزام کارکرد امنیتی عملیات رمزنگاری - رمزگذاری/رمزگشایی (FCS_COP.1(1)) سازگار باشد. هر چند کد احراز هویت پیام مبتنی بر چکیده‌ساز به همراه SHA-256 (HMAC-SHA-256) در این الزام به عنوان مجموعه‌ای از رمزهای قابل انتخاب فهرست شده‌اند، الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS (FCS_TLSC_EXT.1) به طور مؤثری پیاده‌سازی آن را برای انطباق سیستم‌عامل‌ها الزامی می‌سازد. در حال حاضر به منظور انطباق با الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS (FCS_TLSC_EXT.1) و بسته به انتخاب الزام کارکرد امنیتی پیاده‌سازی DTLS (FCS_DTLS_EXT.1)، به SHA-1 نیاز است. SHA-1 در حال حاضر برای انطباق با الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS (FCS_TLSC_EXT.1) مورد نیاز است، اما قدیمی شده است و بهتر است برای اهداف دیگری فراتر از TLS و DTLS مورد استفاده قرار نگیرد.	
۸	تولید بیت تصادفی ۱
سیستم‌عامل باید همه خدمات تولید بیت تصادفی قطعی (DRBG[۴۲]) را مطابق با مورد زیر انجام دهد. [**انتخاب**، حدقل یکی از: *انتشارات ویژه NIST، 800-90A با استفاده از [**انتخاب**: Hash_DRBG (any)، HMAC_DRBG (any)، CTR_DRBG (AES)]،* *FIPS Pub 140-2 پیوست C، X9.31 پیوست ۲,۴ با استفاده از AES*].	

[۴۱] Hash-based Message Authentication Code

[۴۲] deterministic random bit generation

نکته کاربردی ۸: نویسنده هدف امنیتی باید استانداری که با خدمات تولید کننده بیت تصادفی سازگارند انتخاب کند (SP 800-90A یا FIPS 140-2 پیوست C). SP 800-90A شامل سه روش متفاوت برای تولید اعداد تصادفی می‌باشد؛ هر کدام از این‌ها به نوبه خود به مقدمات رمزنگاری زیرین (توابع چکیده‌ساز یا رمزها) وابسته هستند. نویسنده هدف امنیتی تابع استفاده شده را انتخاب خواهد نمود (اگر SP 800-90A انتخاب شده باشد)، و مقدمات رمزنگاری زیرین مشخص استفاده شده در الزام یا در خلاصه مشخصه محصول را می‌گنجاند. در حالی که هر یک از توابع چکیده‌ساز شناسایی شده (SHA-1، SHA-224، SHA-256، SHA-384، SHA-512) برای Hash_DRBG یا HMAC_DRBG مجاز هستند، تنها پیاده‌سازی‌های مبتنی بر استاندارد رمزنگاری پیشرفته برای CTR_DRBG مجازند. توجه داشته باشید که برای پیوست FIPS 140-2 C، در حال حاضر تنها روش توضیح داده شده در بخش ۳ پیوست A.2.4 در ANSI X9.31 تولید کننده عدد تصادفی توصیه شده NIST معتبر است. استفاده از این تولید کننده بیت تصادفی قطعی بعد از سال ۲۰۱۵ بر طبق NIST SP 800-131A غیر مجاز شده است. پروفایل حفاظتی برای انعکاس این موضوع به روز رسانی خواهد شد؛ با این حال، توسعه‌دهندگان بهتر است در اسرع وقت انتقال از این تولید کننده بیت تصادفی قطعی را آغاز کنند.

۹	تولید بیت تصادفی ۲

تولید کننده بیت تصادفی قطعی مورد استفاده سیستم‌عامل باید با یک منبع آنتروپی پیگردی شود که آنتروپی را از مورد زیر جمع می‌کند [**انتخاب**:

منبع پارازیت مبتنی بر نرم‌افزار،

منبع پارازیت مبتنی بر سکو،

] با حداقل [**انتخاب**:

۱۲۸ بیتی،

۲۵۶ بیتی

] از آنتروپی حداقل مساوی با بزرگترین استحکام امنیتی کلیدها و چکیده‌سازهایی که تولید خواهد کرد (مطابق NIST SP 800-57).

نکته کاربردی ۹: برای اولین انتخاب در این الزام، چنانچه منابع پارازیت افزوده‌ای به عنوان ورودی تولید کننده بیت تصادفی قطعی استفاده شده باشند، نویسنده هدف امنیتی "منبع پارازیت مبتنی بر نرم‌افزار" را انتخاب می‌کند.

در انتخاب دوم در این الزام، نویسنده هدف امنیتی تعداد مناسب بیت‌های آنتروپی را که با بزرگترین استحکام امنیتی الگوریتم موجود در هدف امنیتی مطابقت دارد انتخاب می‌کند. استحکام امنیتی در جدول ۲ و ۳ NIST SP 800-57 تعریف شده است. برای مثال، اگر پیاده‌سازی شامل ۲۰۴۸ بیت RSA (استحکام امنیتی ۱۱۲ بیت)، ۱۲۸ AES (استحکام امنیتی ۱۲۸ بیت) و HMAC-SHA-256 (استحکام امنیتی ۲۵۶ بیت)، نویسنده هدف امنیتی ۲۵۶ بیت را انتخاب خواهد نمود.

۱۰	انبارش داده حساس ۱

سیستم‌عامل باید قابلیت کارکردی رمزگذاری داده حساس ذخیره شده در انبارش غیر فرّار را پیاده‌سازی کند و واسط‌هایی برای برنامه‌های کاربردی ارائه دهد تا این قابلیت کارکردی را فراخوانی کنند.

نکته کاربردی ۱۰: : نویسنده هدف امنیتی باید داده حساس را در خلاصه مشخصه محصول مشخص کند، و باید حداقل شامل اعتبارنامه‌ها و کلیدها باشد. واسط‌هایی که برای فراخوانی این قابلیت هستند می‌توانند شکل‌های مختلفی داشته باشند: می‌تواند از یک واسط برنامه‌نویسی برنامه‌کاربردی تشکیل شده باشد، یا به سادگی قراردادهای به خوبی مستند شده‌ای برای دسترسی به اعتبارنامه‌هایی باشد که به عنوان فایل ذخیره شده‌اند.

۱۱	پروتکل سرویس‌گیرنده TLS ۱

سیستم‌عامل باید TLS 1.2 (RFC 5246) را پیاده‌سازی کند که از مجموعه رمزهای زیر پشتیبانی می‌کند:

مجموعه رمزهای اجباری: TLS_RSA_WITH_AES_128_CBC_SHA همانگونه که در RFC 5246 تعریف شده است

مجموعه رمزهای اختیاری : [انتخاب:

TLS_DHE_RSA_WITH_AES_128_CBC_SHA همانگونه که در RFC 5246 تعریف شده است،

TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 همانگونه که در RFC 5246 تعریف شده است،

TLS_DHE_RSA_WITH_AES_256_CBC_SHA همانگونه که در RFC 5246 تعریف شده است،

TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 همانگونه که در RFC 5246 تعریف شده است،

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA همانگونه که در RFC 4492 تعریف شده است،

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 همانگونه که در RFC 5289 تعریف شده است،

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 همانگونه که در RFC 5289 تعریف شده است،

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA همانگونه که در RFC 4492 تعریف شده است،

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 همانگونه که در RFC 5289 تعریف شده است،

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 همانگونه که در RFC 5289 تعریف شده است،

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA همانگونه که در RFC 5289 تعریف شده است،

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 همانگونه که در RFC 5289 تعریف شده است،

TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 همانگونه که در RFC 5246 تعریف شده است،

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA همانگونه که در RFC 4492 تعریف شده است،

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 همانگونه که در RFC 5289 تعریف شده است،

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 همانگونه که در RFC 5289 تعریف شده است،

TLS_RSA_WITH_AES_128_CBC_SHA256 همانگونه که در RFC 5246 تعریف شده است،

TLS_RSA_WITH_AES_256_CBC_SHA همانگونه که در RFC 5246 تعریف شده است،

TLS_RSA_WITH_AES_256_CBC_SHA256 همانگونه که در RFC 5246 تعریف شده است،

هیچ مجموعه مرز دیگری]. **نکته کاربردی ۱۱:** مجموعه رمزهایی که در پیکربندی ارزیابی شده مورد آزمون قرار خواهند گرفت توسط این الزام محدود می‌شوند. نویسنده هدف امنیتی باید مجموعه رمزهای انتخابی را انتخاب کند که پشتیبانی می‌شوند؛ چنانچه هیچ مجموعه رمزی به غیر از مجموعه‌های اجباری پشتیبانی نشد، باید "هیچ مجموعه رمز دیگری" انتخاب شود. ضروری است مجموعه رمزهایی که در یک پیکربندی اجرایی ارزیابی شده بر روی سرور در محیط آزمون قابل استفاده هستند محدود شوند. الگوریتم B مجموعه رمزها که در بالا فهرست شده‌اند (RFC 6460) الگوریتم‌های ترجیحی برای پیاده‌سازی هستند. برای حصول اطمینان از انطباق با RFC 5246 به TLS_RSA_WITH_AES_128_CBC_SHA نیاز است. این الزامات به عنوان نسخه‌های جدید TLS توسط IETF استانداردسازی شده‌اند. اگر هر مجموعه رمزی با استفاده از ECDHE انتخاب شد به FCS_TLSC_EXT.2.1 نیاز است.	
پروتکل سرویس‌گیرنده TLS ۲	**۱۲**
سیستم‌عامل باید بررسی کند که شناسه ارائه شده مطابق با RFC 6125 با شناسه مرجع مطابقت داشته باشد. **نکته کاربردی ۱۲:** قوانین درستی‌سنجی هویت در بخش ۶ RFC 6125 توضیح داده شده‌اند. شناسه مرجع بسته به خدمت سیستم‌عامل توسط کاربر (به طور مثال، واردکردن نشانی وب یا مکان یکنواخت منبع (URL[۴۳]) در یک مرورگر وب یا کلیک کردن روی یک لینک)، با پیکربندی (به طور مثال، پیکربندی نام میل سرور یا سرور احراز هویت)، یا توسط یک برنامه‌کاربردی (به طور مثال، پارامتری از یک واسط برنامه‌نویسی برنامه‌کاربردی) تعیین شده است. بر اساس دامنه منبع شناسه مرجع منحصربه‌فرد و نوع خدمت برنامه‌کاربردی (به طور مثال، HTTP، SIP، LDAP)، سرویس‌گیرنده همه شناسه‌های مرجعی که قابل قبول هستند مانند نام مشترک برای	

[۴۳] Uniform Resource Locator

رشـــته نام موجودیت فعال گواهی و یک نام DNS (حســـاس به حروف بزرگ و کوچک)، نام URI و نام خدمت برای رشـــته نام جایگزین موجودیت فعال ایجاد می‌کند. سرویس‌گیرنده فهرستی از همه شناسه‌های مرجع قابل قبول را با شناسه‌های ارائه شده در گواهی سرور TLS مقایسه می‌کند. روش ارجح برای درستی‌سنجی نام جایگزین موجودیت فعال با استفاده از نام‌های DNS، نام‌های URI، یا نام‌های خدمت می‌باشد. درستی‌سنجی استفاده کننده از نام مشترک برای اهداف سازگاری پس‌سو مورد نیاز است. علاوه بر این، پشتیبانی برای استفاده از آدرس‌های IP در نام موجودیت فعال یا نام جایگزین موجودیت فعال بر خلاف به‌روش‌ها تضعیف شده است اما ممکن است پیاده‌سازی شود. در نهایت توصیه می‌شود سرویس‌گیرنده از ساخت شناسه‌های مرجع استفاده کننده از کاراکترهای عام[۴۴] خودداری کنند. با این حال، اگر شناسه‌های ارائه شده شامل کاراکترهای عام باشد، سرویس‌گیرنده باید به منظور تطبیق از به‌روش‌ها تبعیت کند؛ این به‌روش‌ها در اقدامات تضمین آورده شده‌اند.

۱۳	پروتکل سرویس‌گیرنده TLS ۳

اگر گواهی متناظر معتبر باشد سیستم‌عامل تنها یک کانال قابل اعتماد ایجاد خواهد کرد. **نکته کاربردی ۱۳:** اعتبار با درستی‌سنجی شناسه، مسیر گواهی، تاریخ انقضا و وضعیت ابطال مطابق با RFC 5280 تعیین خواهد شد. اعتبار گواهی باید مطابق با آزمون انجام شده در FIA_X509_EXT.1 مورد آزمون قرار گیرد. در صورتی که گواهی متناظر نامعتبر باشد، این کانال نباید برای اتصالات TLS ایجاد شود.

۶-۳- کلاس حفاظت از داده کاربر

شماره الزام	نام الزام
۱۴	**کنترل‌های دسترسی برای حفاظت از داده کاربر ۱**

[۴۴] wildcard

سیستم‌عامل باید کنترل‌های دسترسی را پیاده‌سازی کند که بتواند مانع دسترسی کاربران غیر ممتاز به فایل‌ها و دایرکتوری‌های متعلق به کاربران دیگر شود. **نکته کاربردی ۱۴:** حفاظت اثربخش با کنترل‌های دسترسی به پیکربندی سامانه نیز بستگی دارد. این الزام بدین منظور طراحی شده است تا اطمینان حاصل کند که، به عنوان مثال، فایل‌ها و دایرکتوری‌های متعلق به یک کاربر در یک سامانه چند کاربره می‌تواند از دسترسی توسط دیگر کاربران در آن سامانه محافظت گردد.
۱۵ **کنترل جریان اطلاعات ۱**
سیستم‌عامل باید [**انتخاب**: *ارائه واسطی که به یک سرویس‌گیرنده شبکه خصوصی مجازی (VPN)*[۴۵] *اجازه حفاظت از همه ترافیک IP را با استفاده از IPsec بدهد،* *ارائه سرویس‌گیرنده شبکه خصوصی مجازی که می‌تواند از همه ترافیک IP با استفاده از IPsec محافظت کند*] به استثنای ترافیک IP مورد نیاز برای ایجاد اتصال شبکه خصوصی مجازی. **نکته کاربردی ۱۵:** به طور معمول، ترافیک مورد نیاز برای ایجاد اتصال شبکه خصوصی مجازی به عنوان ترافیک "سطح کنترل[۴۶]" معرفی شده است در حالیکه ترافیک IP محافظت شده توسط IPsec VPN به عنوان ترافیک "سطح داده[۴۷]" معرفی می‌شود. همه ترافیک "سطح داده" باید از طریق اتصال شبکه خصوصی مجازی جریان داشته باشند و شبکه خصوصی مجازی نباید تونل دو نیم[۴۸] باشد.

[۴۵] Virtual Private Network

[۴۶] Control Plane

[۴۷] Data Plane

[۴۸] Split-tunnel

اگر هیچ سرویس‌گیرنده بومی IPsec معتبر نشده باشد یا سرویس‌گیرنده‌های شبکه خصوصی مجازی طرف سوم هم پیاده‌سازی شوند کنترل جریان اطلاعات مورد نیاز، اولین گزینه‌ای است که باید انتخاب شود. در این موارد محصول، واسط برنامه‌نویسی برنامه‌کاربردی را برای سرویس‌گیرنده‌های شبکه خصوصی مجازی طرف سوم فراهم می‌آورد که به آن‌ها اجازه پیکربندی پشته[۴۹] شبکه محصول را برای انجام کنترل جریان اطلاعات مورد نیاز می‌دهد.

در صورتی که توابع هدف امنیتی سرویس‌گیرنده شبکه خصوصی مجازی بومی پیاده‌سازی کند نویسنده هدف امنیتی باید گزینه دوم را انتخاب کند (IPsec در FTP_ITC_EXT.1 انتخاب شده است). چنانچه سرویس‌گیرنده شبکه خصوصی مجازی بومی باید اعتباردهی گردد (IPsec در FTP_ITC_EXT.1 انتخاب شده است و توابع هدف امنیتی مطابق *بسته توسعه یافته برای سرویس‌گیرنده شبکه‌های خصوصی مجازی* معتبر شده است)، نویسنده هدف امنیتی همچنین باید FDP_IFC_EXT را از این بسته بگنجاند. در آینده، این الزام ممکن است تمایزی بین الزامات فعلی (که موقعی مورد نیاز است که کانال قابل اعتماد IPsec فعال است، همه ترافیک از توابع هدف امنیتی از طریق این کانال مسیردهی شده است) ایجاد کند و گزینه انتخابی داشته باشد که برقراری یک کانال قابل اعتماد IPsec را اجباری کند تا اجازه هرگونه اتصالی توسط توابع هدف امنیتی داده شود.

[۴۹] stack

۶-۴- کلاس مدیریت امنیت

شماره الزام	نام الزام
۱۶	مدیریت رفتار توابع امنیتی ۱

سیستم‌عامل باید قادر به انجام کارکردهای مدیریتی زیر باشد که توسط کاربر کنترل و توسط مدیر سیستم به نحوی که نشان داده شده است باطل می‌شود:

- X: اجباری
- O: اختیاری

کارکرد مدیریتی	مدیر سیستم	کاربر
پیکربندی حداقل طول کلمه‌عبور	O	O
پیکربندی حداقل تعداد نویسه‌های خاص در کلمه‌عبور	O	O
پیکربندی حداقل تعداد نویسه‌های عددی در کلمه‌عبور	O	O
پیکربندی حداقل تعداد نویسه‌های با حروف بزرگ در کلمه‌عبور	O	O
پیکربندی حداقل تعداد نویسه‌های با حروف کوچک در کلمه‌عبور	O	O
فعال یا غیرفعال کردن قفل صفحه نمایش	O	O
پیکربندی وقفه عدم فعالیت قفل صفحه کلید	O	O
پیکربندی وقفه عدم فعالیت اتصال از راه دور	O	O
فعال یا غیرفعال کردن ورودهای غیر احراز اصالت شده به سامانه	X	X
پیکربندی خط‌مشی ممنوعیت تلاش‌های احراز هویت ناموفق از طریق [**انتخاب**: وقفه بین تلاش‌ها، محدود کردن تعداد تلاش‌ها در طول یک دوره زمانی]	O	O
پیکربندی دیواره آتش مبتنی بر میزبان	O	O

پیکربندی نام و یا آدرس سرور دایرکتوری برای اتصال	O	O
پیکربندی نام و یا آدرس سرور مدیریت از راه دور که برای دریافت تنظیمات مدیریتی می‌باشد.	O	O
پیکربندی نام و یا آدرس سرور ممیزی و یا ورود که برای ارسال رکوردهای ممیزی و یا ورود می‌باشد.	O	O
پیکربندی ظرفیت انبارش ممیزی محلی	O	O
پیکربندی قوانین ممیزی	O	O
پیکربندی نام و یا آدرس سرور زمان شبکه	O	O
فعال یا غیرفعال کردن به روز رسانی خودکار نرم‌افزار	O	O
پیکربندی واسط اتصال WiFi	O	O
فعال یا غیرفعال کردن واسط بلوتوث	O	O
پیکربندی واسط‌های USB	O	O
فعال یا غیرفعال کردن [**اختصاص**: فهرستی از دیگر واسط‌های خارجی]	O	O
[**اختصاص**: فهرستی از دیگر توابع مدیریتی که باید توسط توابع هدف امنیتی فراهم گردد]	O	O

نکته کاربردی ۱۶: اصطلاح "کاربر" و "مدیر سیستم" در بخش ۲-۲-۱ تعریف شده است. هدف از این الزام حصول اطمینان از این موضوع است که هدف امنیتی با کارکردهای مدیریتی‌ای ارائه شده است که توسط سیستم‌عامل ارائه گردیده است. این الزام چک فهرست‌های انطباقی برای توسعه‌دهندگان فراهم می‌آورد، از جمله مواردی که به عنوان راهنمای کاربر عملیاتی ارائه شده است به نحوی که در AGD_OPE.1.3C مشخص شده است. تا این جدول را با ارائه مقادیر مختص شرکت برای هر آیتم ارزیابی شده به صورت اهرمی به کار گیرد.

خط‌مشی‌های مدیریت حساب پیچیده، مانند الزامات پیچیده پیچیدگی کلمه‌عبور و ساماندهی حساب‌های موقت، کارکردی از سرورهای دایرکتوری می‌باشند. سیستم‌عامل می‌تواند در چنین مدیریت حساب‌هایی عضو شده و سامانه اطلاعات کلی را برای دستیابی به چنین خط‌مشی‌هایی با اتصال به یک سرور دایرکتوری فعال کند. در مواردی که کاربر و مدیر سیستم هر دو می‌توانند یک تابع مدیریت خاص را کنترل کنند، اگر مدیر سیستم خط‌مشی‌ای تنظیم نکرده باشد کاربر ممکن است مجاز به اجرای آن تابع باشد. نویسنده هدف امنیتی باید از یک "-" (به جای "X") استفاده کند تا جاهایی را که مدیریت ارائه نشده است نشان دهد.

۶-۵- کلاس حفاظت از توابع هدف امنیتی

شماره الزام	نام الزام
۱۷	**کنترل‌های دسترسی ۱**
سیستم‌عامل باید کنترل‌های دسترسی پیاده‌سازی کند که از تغییر موارد زیر توسط کاربران غیر ممتاز ممانعت می‌کند: • هسته و درایورها و ماژول‌های آن • ثبت‌های وقایع ممیزی امنیتی • کتابخانه‌های مشترک • فایل‌های اجرایی سامانه • فایل‌های پیکربندی سامانه [**اختصاص**: موجودیت‌های غیرفعال دیگر]	
۱۸	**کنترل‌های دسترسی ۲**
سیستم‌عامل باید کنترل‌های دسترسی پیاده‌سازی کند که مانع کاربران غیر ممتاز از خواندن موارد زیر می‌شود:	

• ثبت‌های وقایع ممیزی امنیتی • مخازن اعتبارنامه گسترده در سامانه • [اختصاص: موجودیت‌های غیرفعال دیگر]
۱۹ **تصادفی‌سازی چیدمان فضای آدرس ۱**
سیستم‌عامل باید همیشه فرایند مکان‌های حافظه فضای آدرس را به جز برای [**اختصاص**: فهرستی از استثنائات صریح و روشن] تصادفی کند.
۲۰ **حفاظت از سرریز بافر پشته ۱**
سیستم‌عامل باید با حفاظت‌های سرریز بافر مبتنی بر پشته فعال شده کامپایل شود. **نکته کاربردی ۱۷:** انتظار می‌رود که بیشتر سیستم‌عامل، برای گنجاندن هسته، کتابخانه‌های مشترک، و نرم‌افزارهای کاربردی از فروشنده سیستم‌عامل با حفاظت سرریز بافر سیستم‌عامل فعال شده کامپایل گردد.
۲۱ **یکپارچگی راه‌اندازی ۱**
سیستم‌عامل باید یکپارچگی زنجیره راه‌اندازی[۵۰] سر تا سر هسته سیستم‌عامل را بررسی کند و [**انتخاب**: *همه کدهای اجرایی ذخیره شده در رسانه ناپایدار، [**اختصاص**: فهرستی از کدهای اجرایی]،* *هیچ کد اجرایی دیگری*] قبل از اجرای آن با استفاده از [**انتخاب**: *یک امضای دیجیتال با استفاده از کلید نامتقارن حفاظت شده سخت‌افزاری،* *یک چکیده‌ساز حفاظت شده سخت‌افزاری*]

[۵۰] bootchain

نکته کاربردی ۱۸: زنجیره راه‌اندازی سیستم‌عامل توالی از نرم‌افزار است که شامل بار کننده سیستم‌عامل، هسته، درایورها یا ماژول‌های سامانه، و فایل‌های سامانه‌ای است که در نهایت منجر به بارگذاری سیستم‌عامل می‌شود. اولین قسمت از سیستم‌عامل، معمولاً به بارکننده راه‌انداز مرحله اول[۵۱] اشاره دارد که باید توسط سکو بارگذاری شود. ارزیابی یکپارچگی آن که حیاتی است مسئولیت سکو است؛ و بنابراین خارج از دامنه کاربرد این پروفایل حفاظتی است. همه نرم‌افزارهای بارگذاری شده در این مرحله به طور بالقوه تحت کنترل سیستم‌عامل هستند و در دامنه کاربرد هستند.

درستی‌سنجی ممکن است ماهیتاً تراگذر باشد: یک کلید عمومی محافظت شده سخت‌افزاری یا چکیده‌ساز ممکن است برای بررسی کد بارکننده راه‌انداز ناپایداری استفاده شود که شامل کلید یا چکیده‌ساز مورد استفاده توسط بار کننده راه‌انداز برای بررسی کد هسته سیستم‌عامل ناپایدار است، و این خود شامل کلید یا چکیده‌سازی برای بررسی لایه بعدی کد اجرایی و به همین ترتیب تا آخر می‌باشد. با این حال، روشی که سخت‌افزار این کلیدها را ذخیره و محافظت می‌کند خارج از دامنه کاربرد این پروفایل است.

اگر تمام کدهای اجرایی (شامل بار کننده(های) راه‌انداز، هسته، درایورهای افزاره، برنامه‌های کاربردی از قبل بارگذاری شده، برنامه‌های کاربردی بارگذاری شده توسط کاربر، و کتابخانه‌ها) بررسی شوند، "همه کدهای اجرایی ذخیره شده در رسانه ناپایدار" باید انتخاب شوند.

۲۲	یکپارچگی نصب و به‌روزرسانی ۱

سیستم‌عامل باید توانایی بررسی به‌روزرسانی‌ها را برای خود نرم‌افزار سیستم‌عامل فراهم آورد.

نکته کاربردی ۱۹: این الزام درباره توانایی بررسی در دسترس بودن به‌روزرسانی‌های موثق است، در حالیکه که نصب به‌روزرسانی‌های موثق تحت پوشش FPT_TUD_EXT.1.2 قرار دارد.

۲۳	یکپارچگی نصب و به‌روزرسانی ۲

سیستم‌عامل باید به صورت رمزنگاری به روز رسانی‌های موجود برای خود را با استفاده از امضای دیجیتال قبل از نصب با استفاده از طرح مشخص شده در FCS_COP.1(3) تأیید کند.

[۵۱] First-stage bootloader

۲۴	یکپارچگی نصب و به روز رسانی نرم‌افزار برنامه‌کاربردی ۱
سیستم‌عامل باید توانایی بررسی به‌روز رسانی‌ها را برای نرم‌افزار برنامه‌های کاربردی فراهم آورد. **نکته کاربردی ۲۰:** این الزام درباره توانایی بررسی در دسترس بودن به‌روز رسانی‌های موثق است، در حالیکه که نصب عملی چنین به‌روز رسانی‌هایی تحت پوشش FPT_TUD_EXT.2.2 قرار دارد.	
۲۵	یکپارچگی نصب و به روز رسانی نرم‌افزار برنامه‌کاربردی ۲
سیستم‌عامل باید به صورت رمزنگاری به روز رسانی‌های موجود برای برنامه‌های کاربردی را قبل از نصب با استفاده از امضای دیجیتال مشخص شده در FCS_COP.1(3) تأیید کند.	

۶-۶- کلاس تولید داده ممیزی

شماره الزام	نام الزام
۲۶	**تولید داده ممیزی ۱**
سیستم‌عامل باید قادر به تولید رکورد ممیزی از رویدادهای قابل ممیزی زیر باشد: أ. شروع کردن و پایان دادن توابع ممیزی؛ ب. همه رویدادهای قابل ممیزی برای سطح مشخص نشده ممیزی؛ و ج. o رویدادهای احراز هویت (موفقیت / شکست)؛ o استفاده از رویدادهای با امتیاز ویژه، یا قوانین خاص (امنیت موفقیت آمیز یا شکست خورده، ممیزی، و تغییرات پیکربندی)؛	

o رویدادهای تشدید نقش یا امتیاز (موفقیت / شکست)؛ o [انتخاب: *فایل و رویدادهای موجودیت غیرفعال (تلاش‌های موفق و ناموفق برای ایجاد، دسترسی، حذف، تغییر، تغییر مجوز)،* *رویدادهای مدیریت کاربر و گروه (افزودن موفق و ناموفق، حذف، تغییر، غیرفعال کردن،* *رویدادهای دسترسی داده‌های ثبت وقایع و ممیزی (موفقیت / شکست)،* *درستی‌سنجی رمزنگاری نرم‌افزار (موفقیت / شکست)،* *آغاز برنامه‌ها (موفقیت / شکست به طور مثال به واسطه خط‌مشی محدودیت نرم‌افزار)،* *رویدادهای راه‌اندازی مجدد، آغاز مجدد، و خاموش کردن سامانه (موفقیت / شکست)،* *رویدادهای بارگذاری و تخلیه ماژول هسته (موفقیت / شکست)،* *رویدادهای مدیر سیستم یا دسترسی سطح ریشه (موفقیت / شکست)،* *ورودی خط فرمان (موفقیت / شکست)،* ***[اختصاص**: دیگر رویدادهای قابل ممیزی به طور خاص تعریف شده].*]	
۲۷	تولید داده ممیزی ۲
سیستم‌عامل باید هر رکورد ممیزی را با حداقل اطلاعات زیر ثبت نماید: أ. تاریخ و ساعت رویداد، نوع رویداد، شناسه موجودیت فعال (در صورت امکان)، و خروجی (موفقیت یا شکست) رویداد؛ و	

ب. برای هر نوع رویداد ممیزی، بر اساس تعریف رویداد قابل ممیزی از مؤلفه‌های کارکردی گنجانده شده در پروفایل حفاظتی یا هدف امنیتی، [**اختصاص**: دیگر اطلاعات ممیزی مرتبط].

نکته کاربردی ۲۱: اصطلاح موجودیت *فعال* در اینجا فهمیده می‌شود که باید کاربری باشد که فرایند در طرف آن در حال فعالیت است. چنانچه تعاریف رویداد قابل ممیزی‌ای از مؤلفه‌های کارکردی ارائه نشده باشد، هیچگونه اطلاعات مرتبط با ممیزی اضافه‌ای نیاز نیست.

۶-۷- کلاس شناسایی و احراز هویت

شماره الزام	نام الزام
۲۸	**ساماندهی شکست در احراز هویت ۱**

سیستم‌عامل باید زمانی که [**انتخاب**:

*[**اختصاص**: یک عدد صحیح مثبت]،*

یک عدد صحیح مثبت قابل پیکربندی مدیر سیستمی در یک

*[**اختصاص**: طیفی از مقادیر قابل قبول]*

] تلاش احراز هویت ناموفق برای [**انتخاب**:

احراز هویت مبتنی بر نام کاربری و کلمه‌عبور

احراز هویت مبتنی بر نام کاربری و یک پین که کلیدی نامتقارنی انتشار می‌دهد که در انبارش محافظت شده OE ذخیره شده است،

احراز هویت بر اساس گواهی‌های X.509

] در رابطه با [**اختصاص**: فهرستی از رویدادهای احراز هویت] رخ می‌دهد را تشخیص دهد.
۲۹ **ساماندهی شکست در احراز هویت ۲**
هنگامی که تعداد تلاش‌های ناموفق احراز هویت برای یک حساب کاربری برآورده شد، سیستم‌عامل باید [**انتخاب**: *ممنوعیت حساب کاربری، از کار افتادن حساب کاربری، تنظیم مجدد اعتبارنامه اجباری، [**اختصاص**: فهرستی از اقدامات]*] را انجام دهد. **نکته کاربردی ۲۲:** اقدامی که باید اتخاذ شود باید در اختصاص هدف امنیتی ساکن شود و در راهنمای مدیر سیستمی تعریف شود.
۳۰ **ساز و کارهای احراز هویت چندگانه ۱**
سیستم‌عامل باید ساز و کارهای احراز هویت زیر را برای پشتیبانی از احراز هویت کاربر ارائه دهد [**انتخاب**: *احراز هویت بر اساس کلمه‌عبور و نام کاربری،* *احراز هویت بر اساس نام کاربری و پینی که کلید نامتقارن ذخیره شده در انبارش حفاظت شده OEانتشار را می‌دهد،* *احراز هویت بر اساس گواهی‌های X.509*].
۳۱ **اعتبارسنجی گواهی X.509 ۱**
سیستم‌عامل باید قابلیت کارکردی برای بررسی اعتبار گواهی‌ها مطابق قوانین زیر پیاده‌سازی کند: • اعتبارسنجی گواهی RFC 5280 و اعتبارسنجی مسیر گواهی. • مسیر گواهی باید با یک گواهی CA قابل اعتماد پایان پذیرد. • سیستم‌عامل باید مسیر گواهی را با اطمینان از حضور بسط محدودیت‌های اصلی و اینکه پرچم CA برای همه گواهی‌های CA "درست" تنظیم شده است اعتبارسنجی کند.

- سیستم‌عامل باید وضعیت ابطال گواهی را با استفاده از مورد زیر اعتبارسنجی کند [**انتخاب**: *پروتکل وضعیت گواهی بر خط (OCSP[۵۲]) به نحوی که در RFC 2560 مشخص شده است، فهرست ابطال گواهی (CRL[۵۳]) به نحوی که در RFC 5759 مشخص شده است، بسط درخواست وضعیت OCSP TLS (به طور مثال اتصال OCSP) به نحوی که در RFC 6066 مشخص شده است*]
- سیستم‌عامل باید رشته کاربری کلید توسعه یافته را مطابق قوانین زیر اعتبارسنجی کند:
  - گواهی‌های استفاده شده برای به روز رسانی‌های قابل اعتماد و درستی‌سنجی یکپارچگی کد اجرایی باید هدف امضای کد (id-kp 3 با OID 1.3.6.1.5.5.7.3.3) را در رشته کاربری کلید توسعه یافته داشته باشد.
  - گواهی‌های سرور ارائه شده برای TLS باید هدف احراز هویت سرور (id-kp 1 با OID 1.3.6.1.5.5.7.3.1) را در رشته کاربری کلید توسعه یافته داشته باشد.
  - گواهی‌های سرویس‌گیرنده ارائه شده برای TLS باید هدف احراز هویت سرویس‌گیرنده (id-kp 2 با OID 1.3.6.1.5.5.7.3.2) را در رشته کاربری کلید توسعه یافته داشته باشد.
  - گواهی‌های S/MIME ارائه شده برای رمزگذاری ایمیل و امضا باید هدف حفاظتی ایمیل (id-kp 4 با OID 1.3.6.1.5.5.7.3.4) را در در رشته کاربری کلید توسعه یافته داشته باشد.
  - گواهی‌های OCSP ارائه شده برای پاسخ‌های OCSP باید هدف امضای OCSP (id-kp 9 با OID 1.3.6.1.5.5.7.3.9) را در رشته کاربری کلید توسعه یافته داشته باشد.

[۵۲] Online Certificate Status Protocol

[۵۳] Certificate Revocation List

o (شرطی) گواهی‌های سرور ارائه شده برای EST باید هدف مجوز ثبت (RA [۵۴]) CMC (id-kp cmcRA با OID 1.3.6.1.5.5.7.3.28) را در رشته کاربری کلید توسعه یافته داشته باشد. **نکته کاربردی ۲۳:** FIA_X509_EXT.1.1 فهرستی از قوانین اعتبارسنجی گواهی‌ها تهیه می‌کند. نویسنده هدف امنیتی باید انتخاب کند که آیا وضعیت ابطال با استفاده از OCSP تأیید شـده است یا CRLها. FIA_X509_EXT.2 مستلزم آن است که گواهی‌ها برای HTTPS، TLS و DTLS استفاده شوند؛ این استفاده مستلزم آن است که قوانین کاربری کلید توسعه یافته تأیید شده باشند.
۳۲ **اعتبارسنجی گواهی X.509 ۲**
سیستم‌عامل باید تنها در صورتی که بسط محدودیت‌های اصلی حاضر باشند و پرچم CA "درست" تنظیم شده باشد با یک گواهی به عنوان گواهی CA رفتار کند. **نکته کاربردی ۲۴:** این الزام برای گواهی‌هایی به کار می‌رود که توسط توابع هدف امنیتی مورد استفاده و پردازش قرار می‌گیرند و گواهی‌هایی را که ممکن است به عنوان گواهی‌های CA قابل اعتماد اضافه شوند، محدود می‌کند.
۳۳ **احرازهویت گواهی X.509 ۱**
سیستم‌عامل باید از گواهی‌های X.509v3 به نحوی که توسط RFC 5280 تعریف شده است استفاده کند تا احراز هویت TLS و اتصالات [**انتخاب**: *DTLS، HTTPS، **/اختصاص**: پروتکل‌های دیگر/، هیچ پروتکل دیگری*] را پشتیبانی کند.

۶-۸- کلاس کانال‌ها یا مسیرهای قابل‌اعتماد

[۵۴] Registration Authority

شماره الزام	نام الزام
۳۴	**ارتباط کانال قابل اعتماد ۱**
سیستم‌عامل باید از [**انتخاب**: *TLS مطابق FCS_TLSC_EXT.1*، *DTLS مطابق FCS_DTLS_EXT.1*، *IPsec مطابق Extended Package for IPsec VPN Clients*، *SSH مطابق Extended Package for Secure Shell*] برای فراهم آوردن کانال ارتباطی قابل اعتماد بین خود و موجودیت‌های مجاز IT پشتیبانی کننده قابلیت‌های زیر: [**انتخاب**: *سرور ممیز، سرور احراز هویت، سرور مدیریت،* ***/اختصاص****: قابلیت‌های دیگر/*] که منطقاً از کانال‌های ارتباطی دیگر جدا هستند استفاده کند و شناسایی مطمئنی از نقاط پایانی‌اش و محافظت از داده کانال در برابر افشا و آشکارسازی تغییر داده کانال فراهم آورد. **نکته کاربردی ۲۵:** اگر نویسنده هدف امنیتی IPsec را انتخاب کند، توابع هدف امنیتی باید بر اساس *بسته توسعه داده شده سرویس‌گیرنده‌های شبکه خصوصی مجازی IPsec* اعتبارسنجی شده باشد. اگر نویسنده هدف امنیتی SSH را انتخاب کند، توابع هدف امنیتی باید بر اساس *بسته توسعه یافته پوسته امن* اعتبار سنجی شده باشد. نویسنده هدف امنیتی باید الزامات کارکرد امنیتی برای پروتکل کانال قابل اعتماد انتخاب شده در FTP_ITC_EXT.1 را در بدنه اصلی هدف امنیتی بگنجاند.	
۳۵	**مسیر قابل‌اعتماد ۱**

سیستم‌عامل باید یک مسیر ارتباطی بین خود و کاربران دوری فراهم آورد که منطقاً از دیگر مسیرهای ارتباطی دور هستند و شناسایی مطمئنی از نقاط پایانی و حفاظت از داده ارتباط یافته در برابر تغییر و افشا فراهم آورد.	
مسیر قابل‌اعتماد ۲	**۳۶**
سیستم‌عامل باید اجازه [**انتخاب**: *توابع هدف امنیتی، کاربران محلی، کاربران دور*] را برای آغاز ارتباط از طریق مسیر قابل‌اعتماد بدهد.	
مسیر قابل‌اعتماد ۳	**۳۷**
سیستم‌عامل باید مستلزم استفاده از مسیر قابل اعتماد برای همه اقدامات اجرایی از راه دور باشد. **نکته کاربردی ۲۶:** این الزام اطمینان می‌یابد که مدیر سیستمان مجاز از راه دور همه ارتباطات با سیستم‌عامل را از طریق یک مسیر قابل اعتماد آغاز کرده و همه ارتباطات با سیستم‌عامل توسط مدیر سیستمان از راه دور از طریق این مسیر انجام می‌شود. داده گذشته از طریق این کانال ارتباطی قابل اعتماد به شکلی که در FTP_ITC_EXT.1 تعریف شده است رمزگذاری می‌شود. فعالیت‌های تضمین برای این الزام همچنین الزامات آزمون FTP_TRP.1.1 و FTP_TRP.1.2 هستند.	

۷- الزامات تضمین امنیت

اهداف امنیتی در بخش ۴ برای پرداختن به تهدیدات مشخص شده در بخش ۳-۱ ایجاد شده‌اند. الزامات کارکرد امنیت (SFRها) در بخش ۵-۱ نمونه‌های رسمی از اهداف امنیتی هستند. پروفایل حفاظتی الزامات تضمین امنیت (SARها) را به منظور قالب دادن به حدودی می‌شناسد که ارزیاب مستندات را برای ارزیابی کاربردپذیر تشخیص می‌دهد و آزمون‌های مستقلی را انجام می‌دهد.

این بخش فهرستی از مجموعه الزامات تضمین امنیت از قسمت ۳ معیار مشترک تهیه می‌کند که در ارزیابی‌هایی بر اساس این پروفایل حفاظتی مورد نیاز است. اقدامات تضمین منفردی که باید انجام شوند هم در بخش ۵ و هم در این بخش مشخص شده‌اند.

مدل کلی برای ارزیابی سیستم‌عامل‌ها بر اساس اهداف امنیتی نوشته شده برای مطابقت با این پروفایل حفاظتی به شکلی که در ادامه می‌آیند هستند:

بعد از اینکه هدف امنیتی برای ارزیابی مورد تصویب قرار گرفت، افزارگان ارزیابی امنیت فناوری اطلاعات (ITSEF[۵۵])، سیستم‌عامل محیط پشتیبانی کننده فناوری اطلاعات، و راهنمایی‌های کاربری / اجرایی برای سیستم‌عامل، را به دست خواهد آورد. انتظار می‌رود افزارگان ارزیابی امنیت فناوری اطلاعات اقدامات ملزم شده توسط روشگان ارزیابی مشترک (CEM[۵۶]) را برای استاندارد رمزگذاری پیشرفته و ALC SAR انجام دهد. همچنین افزارگان ارزیابی امنیت فناوری اطلاعات اقدامات تضمین موجود در بخش ۵ که به عنوان تفسیری از دیگر الزامات تضمین روشگان ارزیابی مشترک در نظر گرفته شده است که برای فناوری خاص معرفی شده در سیستم‌عامل به کار می‌رود. اقدامات تضمین که در بخش ۵ آمده است تصریحی بر این موضوع ارائه داده است که توسعه‌دهنده به چه چیزهایی نیاز دارد تا نشان دهد که سیستم‌عامل با پروفایل حفاظتی سازگار است.

جدول ۳ الزامات تضمین امنیت

نام کلاس	نام الزام	توضیحات
Development(ADV)	ADV_FSP.1	مشخصات کارکرد ابتدایی
Guidance Documents(AGD)	AGD_OPE.1	راهنمای کاربری
	AGD_PRE.1	راهنمای آماده‌سازی
Tests(ATE)	ATE_IND.2	آزمون مستقل- انطباق
Vulnerability Assessment(AVA)	AVA_VAN.1	تحلیل آسیب‌پذیری
Life cycle Support(ALC)	ALC_CMC.1	برچسب‌گذاری محصول

[۵۵] the Information Technology Security Evaluation Facility

[۵۶] Common Evaluation Methodology

	ALC_CMS.1	پوشش پیکربندی محصول
	ALC_TSU_EXT.1	به‌روز رسانی‌های امنیتی به هنگام
Security Target(ASE)	ASE_CCL.1	ادعاهای انطباق
	ASE_ECD.1	تعریف مؤلفه‌های توسعه یافته
	ASE_INT.1	تعریف هدف امنیت
	ASE_OBJ.2	اهداف امنیت
	ASE_REQ.2	الزامات امنیتی مشتق شده
	ASE_SPD.1	تعریف مشکلات امنیتی
	ASE_TSS.1	توصیف خلاصه هدف ارزیابی

۷-۱- کلاس ارزیابی هدف امنیتی (ASE)

همانگونه که هر اقدام ASE در [متدولوژی ارزیابی مشترک (CEM)] تعریف شده است.

۷-۲- کلاس توسعه (ADV)

اطلاعات در مورد سیستم‌عامل در مستندات راهنما گنجانده شده برای کاربر نهایی و همچنین بخش خلاصه مشخصه محصول هدف امنیتی در دسترس است. توسعه‌دهنده سیستم‌عامل باید با شرح محصول موجود در خلاصه مشخصه محصول که به الزامات کارکردی مرتبط می‌شود موافق باشد. اقدامات تضمین گنجانده شده در بخش ۵-۱ باید اطلاعات کافی را برای تعیین محتوای مناسب برای بخش خلاصه مشخصه محصول به نویسنده هدف امنیتی ارائه دهد.

۷-۲-۱- مشخصات کارکرد ابتدایی (ADV_FSP.1)

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
مشخصات کارکرد ابتدایی **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید مشخصات کارکردی را ارائه کند.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2D)** **شرح مؤلفه:** توسعه‌دهنده باید ارتباطی از مشخصات کارکردی به الزامات کارکرد امنیتی ارائه نماید. **نکته کاربردی:** مشخصات کارکردی دربرگیرنده اطلاعات مستندات راهنمای کاربردی (AGD_OPE) و راهنمای آماده‌سازی (AGD_PRE) و اطلاعاتی که در بخش «خلاصه مشخصات محصول» سند هدف امنیتی ارائه شده است، می‌باشند. با توجه به دلایلی که باید در

	مستندات و بخش «خلاصه مشخصات محصول» 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 نیست.

مؤلفه‌های محتوایی

نام خانواده	عنصر امنیتی
مشخصات کارکرد (ADV_FSP)	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1C)** **شرح مؤلفه:** مشخصات کارکردی باید اهداف و متدهای مورد استفاده برای هر واسط اجرا کننده کارکرد امنیتی[۵۷] و پشتیبان کننده‌ی الزام کارکرد امنیتی[۵۸] توصیف نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2C)** **شرح مؤلفه:**

[۵۷]-SFR-enforcing TSFI

[۵۸]-SFR-supporting TSFI

	مشخصات کارکردی باید تمام پارامترهای مرتبط با هر واسط اجرا کننده کارکرد امنیتی و پشتیبان کننده‌ی الزام کارکرد امنیتی را مشخص نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.3C)** **شرح مؤلفه:** مشخصات کارکردی باید برای دسته‌بندی ضمنی واسط‌های غیر مداخله کننده‌ی الزام کارکرد امنیتی دلایلی را ارائه نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **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

نام خانواده	عنصر امنیتی
مشخصات کارکرد **(ADV_FSP)**	**نام عنصر: مشخصات کارکرد ابتدایی ۱** **شماره مؤلفه: (ADV_FSP.1.1E)**

	شرح مؤلفه: ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام الزامات مؤلفه‌های محتوایی را برآورده می‌نماید.
	نام عنصر: مشخصات کارکرد ابتدایی ۱ **شماره مؤلفه: (ADV_FSP.1.2E)** **شرح مؤلفه:** ارزیاب باید مشخص نماید که مشخصات کارکردی نمونه کامل و دقیقی از الزامات کارکرد امنیتی می‌باشند.

اقدامات تضمین

هیچ اقدامات تضمین مشخصی در رابطه با این الزامات تضمین امنیت وجود ندارد، به جز حصول اطمینان از این موضوع که اطلاعات فراهم شده است. مستندات مشخصات کارکردی برای پشتیبانی از اقدامات ارزیابی توضیح داده شده در بخش ۵-۱ و دیگر اقدامات توضیح داده شده برای سند راهنمای اجرایی، ATE و SAR AVA ارائه شده است. الزامات محتوای اطلاعات مشخصات کارکردی به طور ضمنی با ایمان به دیگر اقدامات تضمین در حال انجام ارزیابی می‌شود؛ اگر ارزیاب به علت عدم وجود اطلاعات واسط کافی قادر به انجام یک اقدام نباشد، بدان معناست که مشخصات کارکردی کافی ارائه نگردیده است.

۷-۳-کلاس مستندات راهنما (AGD)

مستندات راهنما با هدف امنیتی ارائه خواهد شد. راهنمایی‌ها باید در بردارنده توضیحاتی در مورد این موضوع باشد که پرسنل IT چگونه تأیید کنند که محیط عملیاتی می‌تواند نقش خود را برای قابلیت کارکردی امنیتی ایفا کند. مستندات بهتر است در یک سبک غیر رسمی و قابل خواندن برای پرسنل IT باشد. راهنمایی‌ها باید برای هر محیط عملیاتی که محصول به عنوان ادعایی در هدف امنیتی پشتیبانی می‌شود ارائه گردد. این راهنمایی دستورالعمل‌هایی برای نصب موفقیت‌آمیز توابع هدف امنیتی در آن

محیط؛ و دستورالعمل‌هایی برای مدیریت امنیت توابع هدف امنیتی به عنوان یک محصول و به عنوان مؤلفه‌ای از محیط عملیاتی بزرگتر را در بر می‌گیرد. راهنمایی‌های مرتبط با قابلیت کارکرد امنیتی خاص نیز ارائه گردیده است، الزامات در مورد چنین راهنمایی‌هایی در اقدامات تضمین مشخص شده با هر الزامی موجود است.

۷-۳-۱- راهنمای عملیاتی (AGD_OPE.1)

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
راهنمای عملیاتی **(AGD_OPE)**	**نام عنصر: راهنمای عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید راهنمای عملیاتی ارائه نماید. **نکته کاربردی:** راهنمای عملیاتی نباید در یک سند منفرد گنجانده شود. راهنمایی برای کاربران، مدیران سیستم، و توسعه‌دهندگان برنامه‌کاربردی می‌تواند در اسناد یا صفحات وب گسترده شود. بهتر است توسعه‌دهنده به جای تکرار اطلاعات، اقدامات تضمین برای این مؤلفه را به منظور تعیین مشخصاتی از راهنما که ارزیاب آن‌ها را بررسی خواهد کرد تعیین کند. در نتیجه اطلاعات ضروری برای آماده‌سازی راهنمای قابل قبول فراهم خواهد آمد.

مؤلفه‌های محتوایی

نام خانواده	عنصر امنیتی
راهنمای عملیاتی **(AGD_OPE)**	**نام عنصر: راهنمای عملیاتی ۱** **شماره مؤلفه: (AGD_OPE.1.1C)** **شرح مؤلفه:** راهنمای عملیاتی کاربران باید برای هر نقش کاربر، توابع قابل دسترسی کاربر و امتیازاتی که باید در محیط پردازشی امن کنترل شود، از جمله هشدارهای مناسب را شرح دهد. **نکته کاربردی**: کاربر و مدیر سیستم باید در تعریف نقش کاربر در نظر گرفته شود.
	شماره مؤلفه: (AGD_OPE.1.2C) **شرح مؤلفه:** راهنمای عملیاتی کاربر باید شرح دهد که برای هر نقش کاربر، هر کاربر چگونه از واسط‌های موجود ارائه شده توسط سیستم‌عامل به شیوه‌ای امن استفاده کند.
	شماره مؤلفه: (AGD_OPE.1.3C) **شرح مؤلفه:** راهنمای عملیاتی کاربر باید برای هر نقش کاربری، توابع و واسط‌های در دسترس را توضیح دهد، مخصوصاً همه پارامترهای امنیتی تحت کنترل کاربر از جمله مقادیر امنیتی مناسب.

	نکته کاربردی: این بخش از راهنمای کاربر عملیاتی بهتر است به شکل چک فهرستی ارائه گردد که به سرعت توسط پرسنل IT (یا کاربر نهایی، در صورت لزوم) قابل اجرا باشد و برای استفاده در اقدامات انطباق مناسب باشد. در صورت امکان، این راهنما در قالب شرح چک فهرست پیکربندی توسعه پذیر (XCCDF[۵۹]) برای پشتیبانی از خودکارسازی امنیت بیان شود. به صورت حداقلی این راهنمایی باید در قالب ساخت‌یافته‌ای ارائه شود که شامل عنوانی برای هر آیتم پیکربندی، دستورالعمل‌هایی برای دستیابی به پیکربندی امن و هر توجیه مرتبطی باشد.
	شماره مؤلفه: (AGD_OPE.1.4C) **شرح مؤلفه:** راهنمای عملیاتی باید برای هر نقش کاربری، به وضوح هر نوع رویداد مرتبط با امنیتی نسبت به کارکردهای قابل دسترسی کاربر را ارائه دهد که نیاز است انجام شود، از جمله تغییر دادن مشخصه‌های امنیتی موجودیت‌های تحت کنترل توابع هدف امنیتی.
	شماره مؤلفه: (AGD_OPE.1.5C) **شرح مؤلفه:** راهنمای عملیاتی کاربران باید تمام مدهای ممکن عملکرد سیستم‌عامل (شامل عملیات بعد از خرابی و یا خطاهای عملیاتی)، پیامدهای آن‌ها و استنباط‌هایی برای حفظ عملکرد امن را مشخص کند.
	شماره مؤلفه: (AGD_OPE.1.6C) **شرح مؤلفه:**

[۵۹] eXtensible Configuration Checklist Description Format

	راهنمای عملیاتی باید برای هر نقش کاربر، اقدامات امنیتی را شرح دهد که به منظور برآوردن اهداف امنیتی در محیط عملیاتی چنانکه در هدف امنیتی توصیف شده است، باید دنبال شود.
	شماره مؤلفه: (AGD_OPE.1.7C) **شرح مؤلفه:** راهنمای عملیاتی کاربر باید شفاف و قابل‌فهم باشد.

مؤلفه‌های اقدامات ارزیاب

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

اقدامات تضمین

برخی از محتویات راهنمای عملیاتی با اقدامات تضمین در بخش ۵-۱ و ارزیابی سیستم‌عامل مطابق [متدلوژی ارزیابی مشترک (CEM)] تأیید شده‌اند. اطلاعات افزوده زیر نیز مورد نیاز هستند. چنانچه توابع رمزنگاری توسط سیستم‌عامل ارائه شده باشد، راهنمای عملیاتی باید دستورالعمل‌هایی برای پیکربندی موتور رمزنگاری مرتبط با پیکربندی ارزیابی شده سیستم‌عامل را در برگیرد. این راهنما باید هشدارهایی را به مدیر سیستمانی ارائه دهد که از دیگر موتورهای رمزنگاری ارزیابی نشده و آزمایش نشده در طول

ارزیابی معیار مشترک سیستم‌عامل استفاده می‌کنند. مستندات باید فرایند تأیید به روز رسانی برای سیستم‌عامل با تأیید امضای دیجیتال را توصیف نماید که ممکن است توسط سیستم‌عامل یا سکوی زیرین انجام شود. ارزیاب بررسی خواهد کرد که این فرایند شامل مراحل زیر باشد: دستورالعمل‌هایی برای کسب خود به روز رسانی. که باید شامل دستورالعمل‌هایی برای در دسترس ساختن به روز رسانی برای سیستم‌عامل باشد (به طور مثال، قرار دادن در یک دایرکتوری خاص). دستورالعمل‌هایی برای آغاز فرایند به روز رسانی، همچنین تشخیص اینکه آیا فرایند موفق بوده یا خیر. این شامل تولید امضای دیجیتال یا چکیده‌ساز می‌باشد. سیستم‌عامل احتمالاً قابلیت‌های کارکردی امنیتی را شامل می‌شود که در حوزه ارزیابی تحت این پروفایل حفاظتی قرار نمی‌گیرد. راهنمای عملیاتی باید برای مدیر سیستم روشن سازد که کدام قابلیت کارکرد امنیتی تحت پوشش اقدامات ارزیابی قرار دارد.

۷-۳-۲- راهنمای آماده‌سازی (AGD_PRE.1)

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول را همراه با راهنمای آماده‌سازی ارائه نماید. **نکته کاربردی**: همراه با راهنمای عملیاتی، توسعه‌دهنده باید به اقدامات تضمین برای تعیین محتوای موردنیاز با توجه به روش‌های اجرایی آماده‌سازی توجه کند.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
راهنمای آماده‌سازی **(AGD_PRE)**	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1C)** **شرح مؤلفه:** راهنمای آماده‌سازی باید تمام مراحل لازم برای پذیرش امن سیستم‌عامل تحویل داده‌شده مطابق با روش‌های اجرایی تحویل توسعه‌دهنده را شرح دهد.
	شماره مؤلفه: (AGD_PRE.1.2C) **شرح مؤلفه:** راهنمای مقدماتی باید تمام مراحل لازم برای نصب و راه‌اندازی امن سیستم‌عامل و آماده‌سازی امن محیط عملیاتی مطابق با اهداف امنیتی محیط عملیاتی توصیف شده در هدف امنیتی را شرح دهد.

مؤلفه‌های اقدامات ارزیاب

راهنمای آماده-سازی	**نام عنصر: راهنمای آماده‌سازی ۱** **شماره مؤلفه: (AGD_PRE.1.1E)** **شرح مؤلفه:**

(AGD_PRE)	ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.
	شماره مؤلفه: (AGD_PRE.1.2E) **شرح مؤلفه:** ارزیاب باید رویه‌های آماده‌سازی شرح داده شده در سند را بکار ببرد تا تائید کند محصول می‌تواند به صورت امن برای عملیاتی شدن آماده شود.

اقدامات تضمین

همانگونه که در مقدمه بالا نشان داده شد، انتظارات قابل توجهی با توجه به مستندات وجود دارد – مخصوصاً هنگام پیکربندی محیط عملیاتی برای پشتیبانی از الزامات کارکردی سیستم‌عامل. ارزیاب باید بررسی کند تا اطمینان یابد که راهنمای ارائه شده برای سیستم‌عامل به طور کافی همه سکوهای ادعا شده برای سیستم‌عامل در هدف امنیتی را مورد توجه قرار می‌دهد.

۷-۴- کلاس پشتیبانی چرخه حیات (ALC)

در سطح تضمین ارائه شده برای انطباق سیستم‌عامل با این پروفایل حفاظتی، پشتیبانی چرخه حیات محدود به جنبه‌های مشهود کاربر نهایی چرخه حیات زندگی است نسبت به اینکه آزمایش فرایند مدیریت پیکربندی و توسعه فروشنده سیستم‌عامل. این بدین معنا نیست که نقش حیاتی‌ای که اقدامات توسعه‌دهنده در قابلیت اعتماد کلی یک محصول بازی می‌کند تضعیف گردد؛ بلکه، انعکاسی از اطلاعاتی است که باید برای ارزیابی در این سطح تضمین موجود باشد.

۷-۴-۱- برچسب‌گذاری محصول (ALC_CMC.1)

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید محصول و مرجع محصول را ارائه نماید.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی **(ALC_CMC)**	**نام عنصر: برچسب‌گذاری محصول ۱** **شماره مؤلفه: (ALC_CMC.1.1C)** **شرح مؤلفه:** محصول باید با مرجع منحصر به فردی برچسب زده شود. **نکته کاربردی**: اطلاعات مرجع منحصر به فرد عبارت است از: • نام سیستم‌عامل • نسخه سیستم‌عامل • شرح سیستم‌عامل

	• برچسب‌های شناسایی نرم‌افزار (SWID) [۶۰]، در صورت وجود.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
قابلیت‌های پیکربندی (ALC_CMC)	**شماره مؤلفه: (ALC_CMC.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید نماید که اطلاعات ارائه شده تمام مؤلفه‌های محتوایی را برآورده می‌نماید.

اقدامات تضمین

ارزیاب هدف امنیتی را بررسی خواهد کرد تا اطمینان یابد که در برگیرنده یک شناسه (مانند نام یا شماره نسخه محصول) است که به طور خاص نسخه‌ای را مشخص می‌کند که الزامات هدف امنیتی را برآورده می‌سازد. علاوه بر این ارزیاب راهنمایی‌های سند راهنمای اجرایی و نمونه‌های سیستم‌عامل دریافت شده برای آزمون را بررسی می‌کند تا اطمینان حاصل کند که شماره نسخه مطابق با چیزی است که در هدف امنیتی می‌باشد. اگر فروشنده وب سایت تبلیغاتی‌ای برای سیستم‌عامل داشته باشد، ارزیاب اطلاعات موجود در وب سایت را بررسی خواهد کرد تا اطمینان یابد که اطلاعات موجود در هدف امنیتی برای تمایز قائل شدن برای محصول کافی هستند.

۷-۴-۲- پوشش پیکربندی محصول (ALC_CMS.1)

مؤلفه‌های اقدامات توسعه‌دهنده

[۶۰] Software Identification

نام خانواده	عنصر امنیتی
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید فهرستی را برای پیکربندی سیستم‌عامل ارائه دهد

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
حوزه پیکربندی **(ALC_CMS)**	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.2.1C)** **شرح مؤلفه:** فهرست پیکربندی باید شامل موارد ذیل باشد: خود سیستم‌عامل و شواهد ارزیابی موردنیاز الزامات تضمین امنیت.
	شماره مؤلفه: (ALC_CMS.1.1C) **شرح مؤلفه:** فهرست پیکربندی باید به طور منحصربه‌فرد آیتم‌های پیکربندی را شناسایی کند.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
حوزه پیکربندی ***(ALC_CMS)***	**نام عنصر: پوشش پیکربندی محصول ۱** **شماره مؤلفه: (ALC_CMS.2.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات فراهم شده تمام الزامات محتوا و ارائه شواهد را فراهم می‌آورد.

اقدامات تضمین

"شواهد ارزیابی مورد نیاز الزامات تضمین امنیت" در این پروفایل حفاظتی محدود به اطلاعاتی است که در هدف امنیتی همراه با راهنمای ارائه شده برای مدیر سیستمان و کاربران تحت الزامات سند راهنمای اجرایی می‌باشد. با اطمینان از این موضوع که سیستم‌عامل به طور خاص شناسایی شده است و این شناسایی با هدف امنیتی و راهنمایی‌های سند راهنمای اجرایی سازگار است (همانگونه که در اقدام تضمین برای ALC_CMC.1 انجام شده است)، ارزیاب اطلاعات مورد نیاز توسط این مؤلفه را نیز به شکل ضمنی تصدیق خواهد کرد. پشتیبانی از چرخه حیات بیشتر از اینکه بررسی عمیقی از فرایند مدیریت پیکربندی و توسعه سازنده توابع هدف امنیتی ارائه دهد، جنبه‌هایی از چرخه حیات توسعه‌دهنده و دستورالعمل‌هایی برای ارائه دهندگان برنامه‌کاربردی برای افزاره‌های توسعه‌دهنده را هدف قرار داده است. این بدین معنا نیست که نقش حیاتی‌ای که اقدامات توسعه دهنده در قابلیت اعتماد کلی یک محصول بازی می‌کند تضعیف گردد؛ بلکه، انعکاسی از اطلاعاتی است که باید برای ارزیابی موجود باشد.

ارزیاب اطمینان حاصل می‌کند که توسعه دهنده یک یا چند محیط توسعه مناسب برای استفاده در برنامه‌های کاربردی در حال توسعه برای سکوی توسعه دهنده را شناسایی کرده است (در مستندات راهنما برای توسعه‌دهندگان برنامه‌کاربردی با توجه به سکوی مورد هدف). توسعه‌دهنده باید برای هر یک از این محیط‌های توسعه‌ای، اطلاعاتی در مورد نحوه پیکربندی محیط ارائه دهد تا اطمینان حاصل کند که ساز و کارهای محافظت از سر ریز بافر در این محیط(ها) مورد استناد قرار گرفته‌اند (به طور مثال، کامپایلر و پرچم‌های لینک دهنده). همچنین ارزیاب اطمینان می‌یابد که این مستندات در بردارنده نشانه‌ای از این است که آیا چنین محافظت‌هایی به صورت پیش فرض هستند یا اینکه

باید به طور خاص فعال شوند. ارزیاب اطمینان حاصل می‌کند که به صورت منحصر به فرد شناسایی شده است (با توجه به دیگر محصولات از فروشنده توابع هدف امنیتی)، و این مستندات ارائه شده توسط توسعه دهنده در ارتباط با الزامات در این هدف امنیتی مرتبط با توابع هدف امنیتی استفاده کننده از این شناسایی منحصر به فرد است.

۷-۴-۳- به‌روز رسانی‌های امنیتی به هنگام (ALC_TSU_EXT.1)

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
به‌روزرسانی‌های امنیتی به‌هنگام **(ALC_TSU_EXT)**	**نام عنصر: به‌روز رسانی‌های امنیتی به‌هنگام ۱** **شماره مؤلفه: (ALC_TSU_EXT.1.1D)** **شرح مؤلفه:** توسعه‌دهنده در خلاصه مشخصه محصول باید شرحی در مورد نحوه به روز رسانی‌های امنیتی به هنگامی که برای سیستم‌عامل ساخته شده است فراهم آورد. هنگامی که به‌روز رسانی‌ها مشخصه‌های امنیتی یا پیکربندی محصول را تغییر می‌دهند توسعه‌دهنده در خلاصه مشخصه محصول باید شرحی در مورد نحوه اطلاع رسانی به کاربران ارائه دهد.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
به‌روزرسانی‌های امنیتی به‌هنگام	**نام عنصر: به‌روز رسانی‌های امنیتی به‌هنگام ۱** **شماره مؤلفه: (ALC_TSU_EXT.1.1C)**

(ALC_TSU_EXT)	**شرح مؤلفه:** توضیحات باید شامل فرایند ایجاد و توسعه به روز رسانی‌های امنیتی برای نرم‌افزار سیستم‌عامل باشد.
	شماره مؤلفه: (ALC_TSU_EXT.1.1C) **شرح مؤلفه:** توضیحات باید شامل فرایند ایجاد و توسعه به روز رسانی‌های امنیتی برای نرم‌افزار سیستم‌عامل باشد.
	نام عنصر: به‌روز رسانی‌های امنیتی به‌هنگام ۲ **شماره مؤلفه: (ALC_TSU_EXT.1.2C)** **شرح مؤلفه:** توضیحات باید شامل ساز و کارهایی باشد که به صورت عمومی برای گزارش‌دهی مسائل امنیتی مربوط به سیستم‌عامل است. ساز و کار گزارش‌دهی می‌تواند شامل وب سایت‌ها، آدرس‌های ایمیل، و همچنین ابزاری برای حفاظت از ماهیت حساس گزارش باشد (به طور مثال، کلیدهای عمومی که می‌تواند برای رمزگذاری جزئیات یک بهره‌برداری اثبات مفاهیم مورد استفاده قرار گیرد).

مؤلفه‌های ارزیاب

نام خانواده	عنصر امنیتی
به‌روزرسانی‌های امنیتی به‌هنگام **(ALC_TSU_EXT)**	**نام عنصر: به‌روز رسانی‌های امنیتی به‌هنگام ۱** **شماره مؤلفه: (ALC_TSU_EXT.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات ارائه شده تمام الزامات محتوا و ارائه شواهد را فراهم می‌آورد.

اقدامات تضمین

ارزیاب بررسی خواهد کرد که خلاصه مشخصه محصول شامل شرح فرایند به‌روز رسانی امنیتی به هنگام مورد استفاده توسط توسعه‌دهنده برای ایجاد و توسعه به‌روز رسانی‌های امنیتی می‌باشد. ارزیاب بررسی خواهد کرد که این توضیحات کل برنامه‌کاربردی را مورد توجه قرار دهد. ارزیاب همچنین بررسی خواهد کرد که علاوه بر فرایند توسعه‌دهنده سیستم‌عامل، هر گونه فرایندهای طرف سوم هم در توضیحات مورد توجه قرار گرفته شده باشد. ارزیاب همچنین بررسی خواهد کرد که هر ساز و کاری برای گسترش به روزرسانی‌های امنیتی شرح داده شده است.

ارزیاب بررسی خواهد کرد که برای هر ساز و کار گسترش شرح داده شده برای فرایند به‌روزرسانی، خلاصه مشخصه محصول زمانی بین افشای عمومی یک آسیب‌پذیری و دسترس پذیری عمومی به روز رسانی‌های امنیتی را به منظور رفع مشکلات این آسیب‌پذیری‌ها فهرست می‌کند تا هر طرف سوم یا حاملی که در گسترش تأخیر ایجاد می‌کند را شامل شود. ارزیاب تأیید خواهد کرد که این زمان به صورت تعداد یا طیفی از روز بیان شده باشد.

ارزیاب بررسی خواهد کرد این توضیحات شامل ساز و کارهای دسترس‌پذیری عمومی برای گزارش‌دهی مسائل امنیتی انتشار یافته مرتبط با سیستم‌عامل باشد (شامل آدرس ایمیل یا وب سایت). ارزیاب باید بررسی کند که توضیحات این ساز و کارها روشی را برای حفاظت از گزارش با استفاده از کلید عمومی برای رمزگذاری ایمیل یا یک کانال قابل اعتماد برای یک وب سایت در برگیرد.

۷-۵- کلاس آزمون‌ها (ATE)

آزمون برای جنبه‌های عملکردی سیستم و نیز جنبه‌هایی مشخص شده است که از طراحی یا پیاده‌سازی نقاط ضعف بهره می‌برد. آزمون قبلی از طریق خانواده ATE_IND انجام شده می‌شد، در حالیکه آزمون فعلی از طریق خانواده AVA_VAN می‌باشد. در سطح تضمین مشخص شده در این پروفایل حفاظتی، آزمون مبتنی بر قابلیت کارکردی اعلان شده و واسط‌هایی با وابستگی به دسترس‌پذیری اطلاعات طراحی است. یکی از خروجی‌های اصلی فرایند ارزیابی گزارش آزمون مشخص شده در الزامات زیر می‌باشد.

۷-۵-۱- آزمون مستقل – انطباق (ATE_IND.1)

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
آزمون مستقل - انطباق **(ATE_IND)**	**نام عنصر: آزمون مستقل - انطباق ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید سیستم‌عامل را برای آزمون ارائه دهد.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
آزمون مستقل - انطباق **(ATE_IND)**	**نام عنصر: آزمون مستقل – انطباق ۱** **شماره مؤلفه: (ATE_IND.1.1C)** **شرح مؤلفه:** سیستم‌عامل باید برای آزمون مناسب باشد.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
آزمون مستقل - انطباق **(ATE_IND)**	**نام عنصر: آزمون مستقل – انطباق ۱** **شماره مؤلفه: (ATE_IND.1.1D)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات فراهم شده تمام الزامات محتوا و ارائه شواهد را برآورده می‌سازد.
	نام عنصر: آزمون مستقل – انطباق ۲ **شماره مؤلفه: (ATE_IND.1.2E)**

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
	شرح مؤلفه: ارزیاب باید زیر مجموعه‌ای از توابع هدف امنیتی را مورد آزمون قرار دهد تا تأیید کند که توابع هدف امنیتی به نحوی عمل می‌کند که مشخص شده است. **نکته کاربردی**: ارزیاب سیستم‌عامل را روی متداول‌ترین نسخه کاملاً عیب‌یابی شده سکو آزمایش خواهد کرد. **اقدامات تضمین:** ارزیاب یک طرح آزمون و گزارش آماده می‌کند که آزمون جنبه‌های سامانه را مستند می‌کند از جمله هر گونه خرابی یا شکستی در برنامه‌کاربردی در طول آزمون می‌شود. ارزیاب باید علت ریشه‌ای هرگونه شکست برنامه‌کاربردی را تعیین کند و این اطلاعات را در گزارش بگنجاند. طرح آزمون تمام اقدامات آزمون گنجانده شده در [روشگان ارزیابی مشترک (CEM)] و متن اقدامات تضمین این پروفایل حفاظتی را پوشش می‌دهد. در حالی که لازم نیست به ازای هر آزمونی که در اقدامات تضمین فهرست شده است مورد آزمونی داشته باشیم، ارزیاب باید در طرح آزمون مستند کند که هر الزام آزمون کاربرد پذیر در هدف امنیتی تحت پوشش قرار گرفته است. طرح آزمون سکوهایی را که باید آزموده شوند شناسایی می‌کند و برای آن سکوهایی که در طرح آزمون گنجانده نشده‌اند ولی در هدف امنیتی وجود دارند، طرح آزمون دلایلی برای عدم آزمون سکو ارائه می‌دهد. این دلایل باید تفاوت‌های بین سکوهای آزموده شده و سکوهای آزموده نشده را مورد توجه قرار دهد، و استدلالی ارائه دهد که تفاوت‌ها بر آزمون‌هایی که باید انجام شود تأثیری ندارند. تنها ابراز این

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
	موضوع که تغییرات تأثیری ندارند کافی نیست؛ توجیهاتی باید ارائه گردد. در صورتی که تمام سکوهای ادعا شده در هدف امنیتی مورد آزمون قرار گرفتند ارائه منطق و توجیه ضروری نیست. طرح آزمون ترکیبی از هر سکویی که باید مورد آزمون قرار گیرد و هرگونه راه‌اندازی که فراتر از چیزی است که در مستندات سند راهنمای اجرایی موجود است را توصیف می‌کند. باید توجه داشت که انتظار می‌رود ارزیاب برای نصب و راه‌اندازی هر سکویی که یا قسمتی از آزمون یا یک شرط پیش آزمون استاندارد است از مستندات سند راهنمای اجرایی تبعیت کند. این ممکن است شامل درایورها و ابزارهای آزمون مشخص باشد. بهتر است برای هر درایور یا ابزاری، استدلال (و نه فقط یک ادعا) فراهم گردد که ابزار یا درایور بر عملکرد قابلیت کارکردی سیستم‌عامل و سکوی آن تأثیر منفی ندارد. این همچنین شامل پیکربندی موتور رمزنگاری است که باید مورد استفاده قرار گیرد. الگوریتم‌های رمزنگاری پیاده‌سازی شده با این موتور آن‌هایی هستند که در این پروفایل حفاظتی مشخص شده‌اند و توسط پروتکل‌های رمزنگاری در حال ارزیابی (IPsec, TLS) مورد استفاده هستند. طرح آزمون اهداف آزمون سطح بالا و همچنین روش‌های آزمونی را که باید برای رسیدن به آن اهداف دنبال شود تعیین می‌کند. این روش‌های اجرایی شامل نتایج مورد انتظار هستند. گزارش آزمون (که فقط می‌تواند نسخه مشروحی از طرح آزمون باشد) اقداماتی را به تفصیل شرح می‌دهد که باید هنگامی اتفاق بیفتد که روش‌های آزمون اجرا گردیدند، و شامل نتایج واقعی آزمون‌ها باشد. این باید یک حساب تجمعی باشد، بنابراین اگر آزمونی اجرا شد که منجر به شکست شد؛ مقدار ثابتی تعیین می‌شود؛ و پس از اجرای مجدد موفقیت‌آمیز آزمون، گزارش نتیجه "رد" و "پذیرش"(و جزئیات پشتیبانی کننده) را نشان خواهد داد، نه فقط نتیجه "پذیرش" را.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی

۷-۶- کلاس ارزیابی آسیب‌پذیری (AVA)

برای اولین تولید این پروفایل حفاظتی، انتظار می‌رود آزمایشگاه ارزیابی منابع متن باز را مورد بررسی قرار دهد تا آسیب‌پذیری‌هایی را بیابد که در این نوع از محصولات کشف شده‌است. در اغلب موارد، این آسیب‌پذیری‌ها مستلزم پیچیدگی‌ای فراتر از یک مهاجم ابتدایی است. تا زمانیکه ابزار نفوذ ایجاد شود و به صورت یکسان در آزمایشگاه‌های ارزیابی توزیع شود، از ارزیاب انتظار نمی‌رود که این آسیب‌پذیری‌ها را در سیستم‌عامل مورد آزمون قرار دهد. انتظار می‌رود آزمایشگاه‌ها در مورد احتمال آسیب‌پذیری‌های داده شده در مستندات ارائه شده توسط فروشنده اظهارنظر کنند. این اطلاعات در توسعه ابزار آزمون نفوذ و برای توسعه پروفایل‌های حفاظتی آینده مورد استفاده خواهند گرفت.

مؤلفه‌های اقدامات توسعه‌دهنده

نام خانواده	عنصر امنیتی
تحلیل آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: تحلیل آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1D)** **شرح مؤلفه:** توسعه‌دهنده باید سیستم‌عامل را برای آزمون ارائه دهد.

مؤلفه‌های اقدامات محتوایی

نام خانواده	عنصر امنیتی
تحلیل آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: تحلیل آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1C)** **شرح مؤلفه:** سیستم‌عامل باید برای آزمون مناسب باشد.

مؤلفه‌های اقدامات ارزیاب

نام خانواده	عنصر امنیتی
تحلیل آسیب‌پذیری **(AVA_VAN)**	**نام عنصر: تحلیل آسیب‌پذیری ۱** **شماره مؤلفه: (AVA_VAN.1.1E)** **شرح مؤلفه:** ارزیاب باید تائید کند که اطلاعات فراهم شده تمام الزامات محتوا و ارائه شواهد را فراهم می‌آورد.
	نام عنصر: تحلیل آسیب‌پذیری ۲

	شماره مؤلفه: (AVA_VAN.1.2E) **شرح مؤلفه:** ارزیاب باید پژوهشی درباره منابع دامنه عمومی برای شناسایی آسیب‌پذیری‌های بالقوه در سیستم‌عامل انجام دهد. **نکته کاربردی**: منابع دامنه عمومی شامل فرهنگ لغت آسیب‌پذیری‌ها و افشاهای مشترک (CVE[۶۱]) برای آسیب‌پذیری‌های می‌باشد که به صورت عمومی شناخته شده‌اند. منابع دامنه عمومی همچنین شامل سایت‌هایی است که فایل‌ها را به صورت آزاد برای یافتن ویروس‌ها مورد بررسی قرار می‌دهند.
	نام عنصر: تحلیل آسیب‌پذیری ۳ **شماره مؤلفه: (AVA_VAN.1.3E)** **شرح مؤلفه:** ارزیاب باید آزمون نفوذ را بر اساس آسیب‌پذیری‌های بالقوه شناسایی شده انجام دهد تا تعیین کند که سیستم‌عامل در مقابل حملات صورت گرفته توسط مهاجمی که پتانسیل حملات اساسی را در اختیار دارد مقاوم است. **اقدامات تضمین:** ارزیاب گزارشی آماده می‌کند که یافته‌هایش را با توجه به این الزامات مستند می‌کند. این گزارش می‌تواند به طور فیزیکی قسمتی از گزارش آزمون کلی ذکر شده در ATE_IND باشد، یا سند جداگانه‌ای باشد. ارزیاب اطلاعات عمومی را برای یافتن

[۶۱] Common Vulnerabilities and Exposures

	آسیب‌پذیری‌هایی جستجو می‌کند که در برنامه‌های کاربردی مشابه یافت شده است با تمرکز خاص بر پروتکل‌های شبکه که برنامه‌کاربردی از آن استفاده می‌کند و سند اجزا و عبارات آن را قالب‌بندی می‌کند. ارزیاب منابع مشورتی و آسیب‌پذیری‌های یافته شده در گزارش را مستند می‌کند. برای هر آسیب‌پذیری یافته شده، ارزیاب توجیهی با توجه به عدم کاربست پذیری‌اش ارائه می‌دهد، یا اینکه ارزیاب آزمونی را (با استفاده از راهنماهای ارائه شده در ATE_IND) شکل می‌دهد تا اگر مناسب باشد، آسیب‌پذیری را تأیید کند. مناسب بودن با ارزیابی بردار حمله مورد نیاز برای نفع بردن از این آسیب‌پذیری مشخص می‌شود. به عنوان مثال، چنانچه بهره‌برداری از آسیب‌پذیری مستلزم مهات‌های تخصصی و میکروسکوپ الکترونیکی باشد، آزمون مناسب نخواهد بود و توجیه مناسبی باید تنظیم شود.

۸- اقدامات تضمین الزامات کارکرد امنیتی

۸-۱ اقدامات تضمین الزام کارکرد امنیتی تولید کلید رمزنگاری (FCS_CKM.1.1)

ارزیاب اطمینان حاصل خواهد کرد که خلاصه مشخصه محصول[۶۲] اندازه‌های کلید پشتیبانی شده توسط سیستم‌عامل را شناسایی می‌کند. چنانچه نویسنده هدف امنیتی بیش از یک طرح تعیین نمود، ارزیاب برای بررسی این موضوع که خلاصه مشخصه محصول کاربری برای هر طرح را تعیین می‌کند آن را مورد آزمون قرار می‌دهد.

ارزیاب بررسی خواهد نمود که راهنمایی سند راهنمای اجرایی[۶۳] به مدیر سیستم دستور می‌دهد که چگونه سیستم‌عامل را به منظور استفاده از طرح(های) تولید کلید منتخب و اندازه(های) کلید برای تمام استفاده‌های تعریف شده در این پروفایل حفاظتی پیکربندی نماید.

نکته اقدام تضمین: آزمون‌های زیر ممکن است مورد نیاز فروشندگان باشد تا محیط توسعه‌دهنده و ابزار توسعه‌دهنده را که به طور معمول در دسترس کاربران نهایی سیستم‌عامل نیستند مجهز کند.

تولید کلید برای طرح‌های RSA انتشارات استانداردهای پردازش اطلاعات فدرال۴-۱۸۶

ارزیاب پیاده‌سازی تولید کلید RSA را با سیستم‌عامل مورد استفاده در آزمون تولید کلید بررسی خواهد کرد. این آزمون توانایی توابع هدف امنیتی[۶۴] را جهت تولید درست مقادیر برای مؤلفه‌های کلید از جمله درستی‌سنجی عمومی توان e، عوامل اول خصوصی p و q، واحدهای عمومی n و محاسبه توان امضای خصوصی d بررسی می‌کند. تولید زوج کلید ۵ راه (یا روش) را برای تولید فاکتورهای اولیه p و q مشخص می‌کند. این ۵ راه عبارتند از:

۱. اعداد اول تصادفی:

---

[۶۲] TSS

[۶۳] AGD: Administrative guidance document

[۶۴] TSF

- اعداد اول قابل اثبات
- اعداد اول احتمالی

۲. اعداد اول با شرایط:

- اعداد اول p1، p2، q1، q2 و q همه باید اعداد اول قابل اثبات باشند
- اعداد اول p1، p2، q1 و q2 همه باید اعداد اول قابل اثبات باشند و p و q باید اعداد اول احتمالی باشند.
- اعداد اول p1، p2، q1، p، q2 و q باید اعداد اول احتمالی باشند.

برای آزمون روش تولید کلید برای روش اعداد اول قابل اثبات تصادفی و برای همه اعداد اول با روش‌های شرطی، ارزیاب باید روال تولید کلید توابع هدف امنیتی را با داده‌های کافی برای تولید قطعی زوج کلید RSA جستجو کند. این شامل نقطه‌های آغاز[۶۵] تصادفی، توان عمومی کلید RSA ، و طول مطلوب کلید می‌باشد. برای هر طول کلید پشتیبانی شده، ارزیاب بایستی توابع هدف امنیتی‌ای داشته باشد که ۲۵ زوج کلید تولید می‌کند. ارزیاب درستی پیاده‌سازی توابع هدف امنیتی را با مقایسه مقادیر تولید شده توسط توابع هدف امنیتی با آن‌هایی که از یک پیاده‌سازی خوب معلوم تولید شده‌اند بررسی خواهد کرد.

در صورت امکان، روش اعداد اول تصادفی احتمالی نیز به گونه‌ای که در بالا توضیح داده شد باید توسط یک پیاده‌سازی خوب شناخته‌شده[۶۶] تأیید شود. در غیر اینصورت، ارزیاب توابع هدف امنیتی خواهد داشت که ۱۰ زوج کلید برای هر طول کلید پشتیبانی شده nlen تولید می‌کند. و بررسی می‌کند که:

- $n = p.q$،
- p و q اعداد اول احتمالی مطابق با آزمون‌های مایلر – رابین هستند،
- $GCD\ p - 1, e = 1$،
- $GCD\ q - 1, e = 1$،

[۶۵] seed

[۶۶] known good implementation

- $2^{256} \geq e \geq 2^{16}$ و e یک عدد صحیح فرد است،
- $|p - q| > 2^{nlen/2-100}$،
- $p \geq 2^{nlen/2-1/2}$،
- $q \geq 2^{nlen/2-1/2}$،
- $2^{(nlen/2)} < d < LCM(p - 1, q - 1)$،
- $e.d = 1 \bmod LCM(p - 1, q - 1)$.

تولید کلید برای طرح‌های RSA ANSI X9.31-1998

چنانچه توابع هدف امنیتی، طرح ANSI X9.31-1998 را پیاده‌سازی کند، ارزیاب خلاصه مشخصه محصول را بررسی خواهد کرد تا مطمئن شود که چگونگی تولید زوج کلیدها را شرح داده شده است. به منظور نشان دادن اینکه پیاده‌سازی توابع هدف امنیتی با ANSI X9.31-1998 مطابقت دارد، ارزیاب اطمینان حاصل خواهد کرد که خلاصه مشخصه محصول شامل اطلاعات زیر است:

- خلاصه مشخصه محصول باید همه بخش‌های استاندارد را که سیستم‌عامل برآورده می‌کند فهرست کند؛
- برای هر بخش قابل اجرای فهرست شده در خلاصه مشخصه محصول برای همه اظهاراتی که "باید" نیستند (که، "نباید"، "توصیه می‌شود"، "توصیه نمی‌شود" هستند)، اگر سیستم‌عامل چنین گزینه‌هایی را پیاده‌سازی می‌کند باید در خلاصه مشخصه محصول توضیح داده شود. اگر قابلیت‌های کارکردی گنجانده شده در استاندارد با "نباید" یا "توصیه نمی‌شود" نشان داده شده است، خلاصه مشخصه محصول باید دلیل منطقی‌ای برای اینکه چرا این موضوع به صورت معکوس بر خط‌مشی امنیت پیاده‌سازی شده توسط سیستم‌عامل تأثیری نخواهد داشت، ارائه دهد؛
- برای هر بخش کاربرد پذیر پیوست ب، هر حذفیاتی از قابلیت‌های کارکردی مرتبط با اظهارات "باید" یا "توصیه می‌شود" بایستی توضیح داده شود.

تولید کلید برای رمزنگاری منحنی بیضوی (ECC)

آزمون تولید کلید FIPS 186-4 ECC

برای هر خم NIST پشتیبانی شده مثل P-256، P-384 و P-521، ارزیاب برای تولید ۱۰ زوج کلید عمومی یا خصوصی به پیاده‌سازی تحت آزمون (IUT) نیاز خواهد داشت کلید خصوصی باید با استفاده از تولید کننده بیت‌های تصادفی (RBG) تأیید شده تولید شوند. برای تعیین درستی، ارزیاب زوج کلیدهای تولید شده را به تابع درستی سنجی کلید عمومی (PKV) یک پیاده‌سازی خوب معلوم ارسال خواهد کرد.

آزمون درستی سنجی کلید عمومی (PKV) FIPS 1864

برای هر خم NIST پشتیبانی شده مثل P-256، P-384 و P-521، ارزیاب ۱۰ زوج کلید عمومی یا خصوصی را با استفاده از تابع تولید کلید از یک پیاده‌سازی خوب معلوم تولید خواهد کرد و پنج عدد از مقادیر کلیدهای عمومی را به گونه‌ای تغییر خواهد داد که نادرست باشند، پنج مقدار بدون تغییر (به طور مثال، صحیح) باقی خواهد ماند. ارزیاب در پاسخ مجموعه‌ای از مقادیر ده تایی قبول یا شکست را به دست خواهد آورد.

۸-۲ اقدامات تضمین الزام کارکرد امنیتی برقراری کلید رمزنگاری ۱ (FCS_CKM.2.1)

ارزیاب اطمینان حاصل خواهد کرد که طرح‌های برقراری کلید پشتیبانی شده با طرح‌های تولید کلید شناسایی شده در FCS_CKM.1.1 مطابقت دارد. چنانچه هدف امنیتی بیش از یک طرح را مشخص کند، ارزیاب خلاصه مشخصه محصول را به منظور بررسی این موضوع که آیا کاربری هر طرح را مشخص می‌کند یا خیر امتحان خواهد کرد.

ارزیاب بررسی خواهد نمود که راهنمایی سند راهنمای اجرایی به مدیر سیستم دستور می‌دهد که چگونه سیستم‌عامل را به منظور استفاده از طرح(های) برقراری کلید منتخب پیکربندی نماید.

نکته اقدام تضمین: آزمون‌های زیر ممکن است مورد نیاز توسعه‌دهندگان باشد تا دسترسی به سکوی آزمونی را فراهم آورند که به ارزیاب ابزارهایی ارائه می‌دهد که به طور معمول در محصولات مرکز تولید یافت نمی‌شوند.

طرح‌های برقراری کلید

ارزیاب پیاده‌سازی طرح‌های برقراری کلید پشتیبانی شده توسط سیستم‌عامل را با استفاده از آزمون‌های کاربرد پذیر زیر بررسی خواهد کرد.

طرح‌های برقراری کلید SP800-56A

ارزیاب پیاده‌سازی طرح‌های توافق کلید SP800-56A سیستم‌عامل را با استفاده از آزمون‌های کارکرد و اعتبار زیر بررسی خواهد کرد. این آزمون‌های اعتبارسنجی برای هر طرح توافق کلید بررسی خواهد نمود که سیستم‌عامل مؤلفه‌های طرح توافق کلید را مطابق با مشخصات موجود در توصیه‌نامه پیاده‌سازی کرده‌است. این مؤلفه‌ها شامل محاسبه رمزنگاری لگاریتم گسسته (DLC[۶۷]) اعداد اول[۶۸] (مقدار (ارزش) راز به اشتراک گذاشته شده Z) و محاسبه مواد کلیدزنی مشتق شده (DKM[۶۹]) از طریق تابع استخراج کلید (KDF[۷۰]) می‌باشد. چنانچه تأیید کلید پشتیبانی شده باشد، ارزیاب با استفاده از روش‌های آزمونی که در زیر توضیح داده شده است بررسی خواهد کرد که مؤلفه‌های تأیید کلید به درستی پیاده‌سازی شده باشند. این شامل تجزیه مواد کلید زنی مشتق شده، تولید داده‌هایMAC و محاسبه برچسب MAC می‌باشد.

آزمون کارکرد

آزمون کارکرد توانایی سیستم‌عامل را در پیاده‌سازی صحیح طرح‌های توافق کلید بررسی می‌کند. برای اجرای این آزمون، ارزیاب باید بردارهای آزمون را از پیاده‌سازی خوب شناخته‌شده طرح‌های پشتیبانی شده توسط سیستم‌عامل تولید و یا کسب کند. برای هر ترکیب طرح توافق کلید پشتیبانی شده – نقش توافق کلید، نوع تابع استخراج کلید، و در صورت پشتیبانی، ترکیب نقش تأیید کلید – نوع تأیید کلید، آزمون کننده باید ۱۰ مجموعه بردار آزمون تولید کند. مجموعه داده شامل خم تأیید شده NIST (ECC) به ازای هر ۱۰ مجموعه از کلیدهای عمومی می‌باشد. این کلیدها بسته به طرحی که مورد آزمون قرار گرفته است ایستا و زودگذر هستند یا هر دو می‌باشند.

---

[۶۷] discrete logarithm cryptography

[۶۸] primitives

[۶۹] derived keying material

[۷۰] Key Derivation Function

ارزیاب مواد کلیدزنی مشـتق شـده، کلیدهای عمومی متناظر سیستم‌عامل (ایستا و یا زودگذر)، برچسب(های) MAC، و هر ورودی مورد استفاده در تابع استخراج کلید مانند دیگر اطلاعات رشته OI و رشته‌های شناسه سیستم‌عامل را به دست خواهد آورد.

چنانچه سیستم‌عامل از تابع استخراج کلید تعریف شده در SP 800-56A استفاده نکرد، ارزیاب تنها کلیدهای عمومی و مقادیر چکیده‌ساز شده را از رازهای مشترک به دست خواهد آورد.

ارزیاب صحت پیاده‌سازی توابع هدف امنیتی از یک طرح داده شده را با استفاده از یک پیاده‌سازی خوب معلوم برای محاسبه مقدار راز مشترک، استخراج مواد کلیدزنی، و مقایسه مقادیر چکیده‌ساز یا برچسب‌های MAC های تولید شده از این مقادیر بررسی خواهد نمود.

چنانچه تأیید کلید پشتیبانی شده باشد، سیستم‌عامل باید مراحل بالا را برای هر الگوریتم تأیید شده MAC پیاده‌سازی شده اجرا کند.

آزمون اعتبار

آزمون اعتبار توانایی سیستم‌عامل را در به رسمیت شناختن نتایج توافق کلید معتبر و نامعتبر بخش دیگر با یا بدون تأیید کلید بررسی می‌کند. برای انجام این آزمون، ارزیاب فهرستی از توابع رمزنگاری پشتیبان را به دست خواهد آورد که در پیاده‌سازی توافق کلید SP800-56A برای تعیین خطاهایی که سیستم‌عامل بهتر است قادر به تشخیص آن‌ها موجود باشد. ارزیاب مجموعه‌ای ۳۰ تایی ار بردارهای آزمون را تولید می‌کند که شامل مجموعه داده از جمله مقادیر پارامتر دامنه یا خم‌های تأیید شده NIST، کلیدهای عمومی ارزیاب، زوج کلیدهای خصوص یا عمومی سیستم‌عامل، برچسب MAC، و هر ورودی مورد استفاده در تابع استخراج کلید مانند اطلاعات دیگر و رشته‌های شناسه سیستم‌عامل می‌باشد.

ارزیاب خطایی را در برخی از بردارهای آزمون تزریق خواهد کرد تا آزمایش کند که آیا سیستم‌عامل نتایج توافق کلید نامعتبر را که ناشی از نادرست بودن رشته‌های زیر است تشخیص می‌دهد: مقدار راز مشترک Z، مواد کلیدزنی مشتق شده، دیگر رشته‌های اطلاعاتی OI، داده‌هایی که باید MAC شوند، یا برچسب MAC تولید شده. اگر سیستم‌عامل اعتبار سنجی کلید عمومی جزئی (تنها ECC) یا کامل را در برگیرد، ارزیاب به صورت جداگانه خطاها را در دو قسمت کلیدهای عمومی ایستا، دو قسمت کلیدهای عمومی زود

گذر و کلیدهای خصوصی ایستای سیستم‌عامل تزریق می‌کند تا اطمینان یابد که سیستم‌عامل خطاها را در تابع اعتبارسنجی کلید عمومی و یا تابع اعتبارسنجی کلید جزئی (تنها در ECC) تشخیص می‌دهد. حداقل دو بردار آزمون باید بدون تغییر باقی بمانند و بنابراین بهتر است منجر به توافق کلید معتبر شود (توصیه می‌شود آن‌ها قبول شوند). سیستم‌عامل باید از این بردارهای آزمون تغییر کرده استفاده کند تا طرح توافق کلید را با استفاده از پارامترهای متناظر تقلید کند. ارزیاب نتایج سیستم‌عامل را با نتایج استفاده شده در یک پیاده‌سازی خوب معلوم مقایسه خواهد کرد تا بررسی کند که سیستم‌عامل این خطاها را تشخیص می‌دهد.

طرح برقراری کلید SP800-56B

ارزیاب بررسی خواهد کرد که آیا خلاصه مشخصه محصول سیستم‌عامل در طرح‌های برقراری کلید مبتنی بر RSA خواه به عنوان یک فرستنده، یک گیرنده، و یا هر دو عمل کند توضیح می‌دهد.

اگر سیستم‌عامل به عنوان یک فرستنده عمل کند، اقدامات تضمین زیر بایستی انجام شود تا از این موضوع اطمینان حاصل شود که عملکرد مناسب هر سیستم‌عامل با ترکیبی از طرح برقراری کلید مبتنی بر RSA پشتیبانی می‌شود:

برای انجام این آزمون، ارزیاب بردار آزمون را از یک پیاده‌سازی خوب معلوم از طرح‌های پشتیبانی شده سیستم‌عامل تولید و یا کسب خواهد نمود. برای هر ترکیبی از طرح برقراری کلید پشتیبانی شده و گزینه‌های انتخابی آن (همراه با یا بدون تأیید کلید اگر پشتیبانی شده باشد، برای هر تابع MAC تأیید کلید پشتیبانی شده اگر تأیید کلید پشتیبانی شده باشد، و برای هر تابع تولید الگوی[۷۱] پشتیبانی شده اگر KTS-OAEP پشتیبانی شده باشد)، آزمونگر باید مجموعه ۱۰ تایی از بردارهای تست را تولید کند. هر بردار تست باید شامل کلید عمومی RSA، مواد کلیدزنی متن خام، و هر پارامتر ورودی افزوده‌ای در صورت امکان، کلید MAC و برچسب MAC در صورتی که تأیید کلید گنجانده شده است، و متن رمز خروجی باشد. برای هر بردار آزمون، ارزیاب باید عملیات رمزنگاری برقراری کلید را بر روی سیستم‌عامل با همان

[۷۱] Mask: یک کلمه ماشینی حاوی الگوئی از بیت‌ها بایت‌ها یا کاراکترها که برای استخراج یا گزینش قسمت‌هایی از کلمات ماشینی دیگر بکار برده می‌شود.

ورودی‌ها انجام دهد (در مواردی که تأیید کلید گنجانده شده است، آزمون باید به جای کلید MAC که به صورت تصادفی تولید شده است و در عملیات عادی استفاده می‌شود از کلید MAC بردار آزمون استفاده کند) و اطمینان حاصل کند که متن رمز خروجی معادل متن رمز در بردار آزمون است.

اگر سیستم‌عامل به عنوان یک گیرنده عمل کند، اقدامات تضمین زیر باید برای حصول اطمینان از عملکرد مناسب هر سیستم‌عامل پشتیبانی شده در ترکیبی از طرح برقراری کلید مبتنی بر RSA انجام شود:

برای انجام این آزمون، ارزیاب بردار آزمون را از یک پیاده‌سازی خوب معلوم از طرح‌های پشتیبانی شده سیستم‌عامل تولید و یا کسب خواهد نمود. برای هر ترکیبی از طرح برقراری کلید پشتیبانی شده و گزینه‌های انتخابی آن (همراه با یا بدون تأیید کلید اگر پشتیبانی شده باشد، برای هر تابع MAC تأیید کلید پشتیبانی شده اگر تأیید کلید پشتیبانی شده باشد، و برای هر تابع تولید الگوی پشتیبانی شده اگر KTS-OAEP پشتیبانی شده باشد)، آزمونگر باید مجموعه ۱۰ تایی از بردارهای تست را تولید کند. هر بردار تست باید شامل کلید خصوصی RSA، مواد کلیدزنی متن خام، و هر پارامتر ورودی افزوده در صورت امکان، برچسب MAC در مواردی که تأیید کلید گنجانده شده است، و متن رمز خروجی باشد. برای هر بردار آزمون، ارزیاب عملیات رمزنگاری برقراری کلید را بر روی سیستم‌عامل انجام خواهد داد و اطمینان حاصل می‌کند که مواد کلیدزنی متن خام خروجی معادل مواد کلیدزنی متن خام در بردار آزمون است. در مواردی که تأیید کلید گنجانده شده است، ارزیاب باید مراحل تأیید کلید را انجام دهد و اطمینان حاصل کند که برچسب MAC خروجی معادل برچسب MAC در بردار تست می‌باشد.

ارزیاب اطمینان حاصل خواهد کرد که خلاصه مشخصه محصول توضیح می‌دهد که چگونه سیستم‌عامل با خطاهای رمزگشایی سر و کار دارد. بر طبق انتشارات ویژه NIST؛ 800-56B سیستم‌عامل نباید خطای خاصی را که رخ داده است، حتی از طریق محتویات هیچ پیام خطای خارج شده یا وارد شده یا از متغیرهای زمانبندی بر جای بگذارد. اگر KTS-OAEP پشتیبانی شود، ارزیاب مقادیر متن رمز ساختگی جداگانه‌ای ایجاد خواهد کرد که هر یک از سه بررسی خطای رمزگشایی توضیح داده شده در بخش ۷,۲,۲,۳ انتشارات ویژه NIST؛ 800-56B را شروع خواهد کرد و اطمینان حاصل می‌کند که هر تلاش رمزگشایی منجر به یک خطا خواهد شد، و اطمینان می‌یابد که پیام خطاهای وارد شده یا خارج شده برای هر یک یکسان است. اگر KTS-KEM-KWS پشتیبانی شود، ارزیاب مقادیر متن رمز ساختگی جداگانه‌ای ایجاد خواهد کرد که هر یک از سه بررسی

خطای رمزگشایی توضیح داده شده در بخش ۷,۲,۳,۳ انتشارات ویژه NIST؛ 800-56B را شروع خواهد کرد و اطمینان حاصل می‌کند که هر تلاش رمزگشایی منجر به یک خطا خواهد شد، و اطمینان می‌یابد که پیام خطاهای وارد شده یا خارج شده برای هر یک یکسان است.

۸-۳ اقدامات تضمین الزام کارکرد امنیتی تخریب کلید رمزنگاری توسعه‌یافته ۱ (FCS_CKM_EXT.3.1)

ارزیاب برای حصول اطمینان از اینکه خلاصه مشخصه محصول هر نوع ماده کلید و منشأ آن و مکان انبارش را فهرست می‌کند آن را بررسی خواهد کرد. ارزیاب بررسی خواهد کرد که خلاصه مشخصه محصول توضیح دهد که کی هر نوع ماده کلید پاک شده است. ارزیاب برای هر موقعیت پاکسازی کلید نرم‌افزار، آزمون زیر را تکرار خواهد کرد.

- **آزمون** ۱: ارزیاب از ترکیب مناسبی از محیط عملیاتی تخصصی شده و ابزار توسعه (برنامه‌های اشکال‌زدائی، شبیه‌سازها و غیره) برای محصول استفاده خواهد کرد و محصول آماده‌سازی شده را برای آزمون کلیدهایی می‌سازد که به درستی پاک شده‌اند، از جمله همه نسخه‌های میانجی کلید که ممکن است در طول پردازش رمزنگاری عادی با آن کلید به صورت داخلی توسط محصول ایجاد شده باشند. پیاده‌سازی محصول رمزنگاری‌شده در نرم‌افزار باید بارگذاری شده باشد و تحت یک برنامه اشکال زدائی برای انجام چنین آزمون‌هایی اجرا شود. ارزیاب مراحل زیر را برای هر کلیدی که سوژه پاکسازی است انجام می‌دهد و شامل نسخه‌های میانجی کلیدهایی که در ادامه رمزگذاری توسط محصول هستند می‌باشد:
  ۱- بارگذاری محصول آماده‌سازی شده ساخته شده تحت یک برنامه اشکال زدائی.
  ۲- ثبت مقدار کلید در محصول که موضوع پاکسازی است.

۳- واداشتن محصول برای انجام پردازش رمزنگاری عادی با کلید از مرحله ۱#.

۴- واداشتن محصول برای پاک کردن کلید.

۵- واداشتن محصول برای توقف اجرا اما نه خروج.

۶- واداشتن محصول برای رونوشت گرفتن از کل حافظه محصول به یک فایل دودویی.

۷- جستجوی محتوای فایل باینری ساخته شده در مرحله ۴# برای نمونه مقادیر کلید معلوم از مرحله ۱#.

آزمون در صورتی موفق می‌شود که هیچ نسخه‌ای از کلید از مرحله ۱# در مرحله ۷# بالا یافت نشود و در غیر اینصورت با شکست روبرو می‌شود.

ارزیاب این آزمون را بر روی همه کلیدها انجام خواهد داد، از جمله آن‌هایی که در ادامه رمزنگاری به وجود آمده‌اند، تا اطمینان حاصل شود که نسخه‌های میانجی پاک شده‌اند.

۴-۸ اقدامات تضمین الزام کارکرد امنیتی عملیات رمزنگاری - رمزگذاری/رمزگشایی ۱ ((FCS_COP.1.1(1))

ارزیاب بررسی می‌کند که آیا مستندات سند راهنمای اجرایی دستورالعمل‌های مورد نیاز برای پیکربندی سیستم‌عامل در استفاده از مدها و اندازه‌های کلید مورد نیاز را در بر می‌گیرد یا خیر. ارزیاب همه دستورالعمل‌هایی که برای پیکربندی سیستم‌عامل به حالت مناسب مشخص شده است را اجرا خواهد کرد. ارزیاب همه آزمون‌های زیر را برای هر الگوریتم پیاده‌سازی شده توسط سیستم‌عامل و استفاده شده برای برآوردن الزامات این پروفایل حفاظتی انجام خواهد داد:

آزمون‌های پاسخ معلوم AES-CBC

چهار آزمون پاسخ معلوم (KATs[۷۲]) در زیر توضیح داده شده است. در همه آزمون‌های پاسخ معلوم، متن خام، متن رمز؛ و مقادیر بردار اولیه[۷۳] باید بلوک‌های ۱۲۸ بیتی باشند. نتایج حاصل از هر آزمون ممکن است مستقیماً توسط ارزیاب به دست آید یا با دادن ورودی‌ها به عملگر و دریافت نتایج در پاسخ به دست آیند. برای تعیین درستی، ارزیاب مقادیر حاصل را با آن‌هایی که از طریق ارسال همان مقادیر در یک اجرای خوب معلوم به دست آمده است، مقایسه خواهد کرد.

- **آزمون پاسخ معلوم ۱:** برای آزمون قابلیت کارکردی رمزگذاری AES-CBC، ارزیاب مجموعه‌ای از ۱۰ مقدار متن خام را توزیع خواهد کرد و مقدار متن رمزی را کسب می‌کند که از رمزگذاری AES-CBC متن خام داده شده با استفاده از یک مقدار کلید از تمام صفر و یک بردار اولیه از تمام صفر در به دست آمده است. پنج تا از مقادیر متن رمز باید یک کلید ۱۲۸ بیتی تمام صفر باشد، و پنج تای دیگر باید با کلید ۲۵۶ بیتی تمام صفر رمز گذاری شوند. برای آزمون قابلیت کارکردی رمزگشایی AES-CBC، ارزیاب همان تستی که برای رمزگذاری انجام داده‌است با استفاده از ۱۰ مقدار متن رمز به عنوان ورودی و رمز گشایی AES-CBC انجام خواهد داد.
- **آزمون پاسخ معلوم ۲:** برای آزمون قابلیت کارکردی رمزگذاری AES-CBC، ارزیاب مجموعه‌ای از ۱۰ مقدار کلید را توزیع خواهد کرد و مقادیر متن رمز حاصل از رمزگذاری AES-CBC یک متن خام تمام صفر با استفاده از مقدار کلید داده شده و یک بردار اولیه تمام صفر از بدست می‌آورد. پنج تا از مقادیر متن رمز باید یک کلید ۱۲۸ بیتی باشد، و پنج تای دیگر باید با کلید ۲۵۶ بیتی باشند. برای آزمون قابلیت کارکردی رمزگشایی AES-CBC، ارزیاب همان تستی که برای رمزگذاری انجام داده‌است را با استفاده از یک مقدار متن رمز تمام صفر به عنوان ورودی و رمز گشایی AES-CBC انجام خواهد داد.
- **آزمون پاسخ معلوم ۳:** برای آزمون قابلیت کارکردی رمزگذاری AES-CBC، ارزیاب دو مجموعه از مقادیر کلیدی که در زیر توضیح داده شده را توزیع خواهد کرد و مقادیر متن رمز حاصل از رمزگذاری استاندارد رمزگذاری پیشرفته یک متن خام تمام صفر با استفاده از مقدار کلید داده شده و یک بردار اولیه تمام صفر از بدست

[۷۲] Known Answer Tests

[۷۳] IV: Initialization vector

می‌آورد. مجموعه اول کلیدها باید ۱۲۸ کلید ۱۲۸ بیتی داشته باشد، و مجموعه دوم باید ۲۵۶ کلید ۲۵۶ بیتی داشته باشد. کلید i در هر مجموعه باید برای i در [1,N]، در سمت چپ باید i بیت یک داشته باشد و در سمت راست N-i بیت صفر باشند. برای آزمون قابلیت کارکردی رمزگشایی AES-CBC، ارزیاب دو مجموعه کلید و زوج مقدار متن رمز توضیح داده شده در زیر را توزیع خواهد کرد و و مقادیر متن خامی که از رمزگشایی AES-CBC از متن رمز داده شده با استفاده از کلید داده شده و یک بردار اولیه تمام صفر به دست خواهد آورد. سری اول زوج‌های متن رمز یا کلید باید ۱۲۸ زوج متن رمز یا کلید ۱۲۸ بیتی داشته باشند، و سری دوم زوج‌های متن رمز یا کلید باید ۲۵۶ زوج متن رمز یا کلید ۲۵۶ بیتی داشته باشند. کلید i در هر مجموعه باید برای i در [1,N]، در سمت چپ i بیت یک و در سمت راست N-i بیت صفر داشته باشد، مقدار متن رمز در هر زوج باید مقداری باشد که وقتی کلید متناظر آن رمزگشایی می‌شود متن خام تمام صفری حاصل شود.

- **آزمون پاسخ معلوم ۴:** برای آزمون قابلیت کارکردی رمزگذاری AES-CBC، ارزیاب مجموعه‌ای از ۱۲۸ مقدار متن خام را که در زیر توضیح داده شده است توزیع خواهد کرد و دو مقدار متن رمزی که به ترتیب از رمزگذاری AES-CBC یک متن خام داده شده با استفاده از مقدار کلید ۱۲۸ بیتی تمام صفر با یک بردار اولیه تمام صفر و با استفاده از مقدار کلید ۲۵۶ بیتی تمام صفر با یک بردار اولیه تمام صفر حاصل می‌شود، بدست می‌آورد. مقدار متن خام i در هر مجموعه باید برای i در [1,128]، در سمت چپ i بیت یک و در سمت راست 128-i بیت صفر داشته باشد.

برای آزمون قابلیت کارکردی AES-CBC، ارزیاب همان آزمونی را که برای رمزگذاری انجام داده است با استفاده از مقادیر متن رمز به همان شکل متن خام در آزمون رمزگذاری به عنوان ورودی و رمزگشائی AES-CBC انجام خواهد داد.

آزمون پیام چند بلوکی AES-CBC

ارزیاب قابلیت رمزنگاری را با رمزنگاری یک پیام i بلوکی که درآن $10 \geq i > 1$ است، آزمایش خواهد کرد. ارزیاب یک کلید، یک بردار اولیه و یک پیام متن خام با طول i قالب انتخاب خواهد نمود و با استفاده از مدی که باید آزموده شود، با کلید و بردار اولیه انتخابی پیام را رمزگذاری خواهد نمود. متن رمز باید با نتایج حاصل از رمزگذاری همان پیام متن خام با همان کلید و بردار اولیه استفاده شده در یک پیاده‌سازی خوب معلوم مقایسه گردد. ارزیاب قابلیت کارکردی رمزگشائی برای هر مد را نیز با رمزگشائی

یک پیام i بلوکی که درآن $1 < i \leq 10$ است خواهد آزمود. ارزیاب یک کلید، یک بردار اولیه و یک پیام متن رمز با طول i قالب را انتخاب خواهد نمود و با استفاده از مدی که باید آزموده شود، با کلید و بردار اولیه انتخابی پیام را رمزگشائی خواهد نمود. متن خام باید با نتیجه رمزگشائی همان پیام با همان خام با همان کلید و بردار اولیه استفاده شده در یک پیاده‌سازی خوب معلوم مقایسه گردد.

آزمون‌های مونت کارلو AES-CBC

ارزیاب قابلیت رمزگذاری را با استفاده از مجموعه‌ای از ۲۰۰ متن خام، بردار اولیه و کلید ۳ تایی آزمون خواهد کرد. ۱۰۰ تا از این‌ها باید از کلیدهای ۱۲۸ بیتی استفاده کنند و ۱۰۰ تای مابقی از کلیدهای ۲۵۶ بیتی. مقادیر متن خام و بردار اولیه باید قالب‌های ۱۲۸ بیتی باشند. برای هر ۳ تایی باید ۱۰۰۰ تکرار به شرح زیر اجرا گردد:

```
#input: PT, IV, Key
  For i=1 to 1000:
    If i ==1:
      CT[1]=AES-CBC-Encrypt (Key, IV, PT)
      PT=IV
    Else:
      CT[i]=AES-CBC-Encrypt (Key, PT)
      PT=CT[i-1]
```

متن رمز محاسبه شده با ۱۰۰۰ امین تکرار (به طور مثال CT[1000]) نتیجه آزمایش است. این نتیجه باید با نتیجه اجرای ۱۰۰۰ تکرار با همان مقادیر با استفاده از یک پیاده‌سازی خوب معلوم مقایسه گردد.

ارزیاب قابلیت کارکردی رمزگشائی را با استفاده از همان آزمونی که برای رمزگذاری استفاده شده، با تبادل CT و PT و جایگذاری AES-CBC-Encrypt با AES-CBC-Decrypt انجام خواهد داد.

آزمون‌های مونت کارلو AES-GCM

ارزیاب قابلیت کارکردی رمزگذاری احراز اصالت شده AES-GCM را برای هر ترکیبی از طول پارامترهای ورودی زیر خواهد آزمود:

- کلید های ۱۲۸ بیتی و ۲۵۶ بیتی
- دو طول متن خام. یکی از طول‌های متن خام بایستی در صورت پشتیبانی عدد صحیح غیر صفر و مضربی ۱۲۸ بیتی باشد. طول متن رمز دیگر در صورت پشتیبانی نباید عدد صحیح و مضربی ۱۲۸ بیتی باشد.
- سه طول AAD. یکی از طول‌های AAD باید در صورت پشتیبانی صفر باشد. یکی از طول‌های AAD باید در صورت پشتیبانی عدد صحیح غیر صفر و مضربی ۱۲۸ بیتی باشد. یکی از طول‌های AAD در صورت پشتیبانی نباید عدد صحیح و مضربی ۱۲۸ بیتی باشد.
- دو طول بردار اولیه. اگر بردار اولیه ۹۶ بیتی پشتیبانی شود، باید یکی از دو طول بردار اولیه تست شده ۹۶ بیت باشد.

ارزیاب قابلیت کارکردی رمزگذاری را با استفاده از مجموعه‌ای از ۱۰ کلید، متن خام، AAD، و بردارهای اولیه چندتایی برای هر ترکیبی از طول پارامترهای بالا خواهد آزمود و مقدار متن رمز و برچسبی که نتیجه رمزگذاری احراز اصالت شده AES-GCM می‌باشد را به دست خواهد آورد. هر طول برچسب پشتیبانی شده باید برای هر مجموعه ۱۰ تایی حداقل یکبار آزمون شود. مقدار بردار اولیه توسط ارزیاب یا پیاده‌سازی آزموده شده معلومی تأمین خواهد شد.

ارزیاب قابلیت کارکردی رمزگشائی را با استفاده از یک مجموعه از ۱۰ کلید، متن رمز، برچسب، AAD، و بردار اولیه پنج تایی برای هر ترکیبی از طول پارامترهای بالا آزمایش خواهد کرد و نتیجه قبول / رد از احراز هویت و در صورت قبولی متن خام رمزگشایی شده‌ای بدست می‌آورد.

نتایج حاصل از هر آزمونی ممکن است به صورت مستقیم توسط ارزیاب بدست آید و یا با تأمین ورودی به مجری و دریافت نتایج در پاسخ حاصل شود. ارزیاب برای تعیین درستی، مقادیر نتیجه را با آن‌هایی که از ارسال همان ورودی‌ها در یک پیاده‌سازی خوب معلوم به دست آمده‌است مقایسه خواهد کرد.

آزمون‌های AES-CCM

ارزیاب قابلیت کارکردی تولید رمزنگاری و درستی سنجی رمزگشائی AES-CCM را برای پارامترهای ورودی و طول برچسب‌های زیر مورد آزمون قرار خواهد داد:

- کلید های ۱۲۸ بیتی و ۲۵۶ بیتی
- دو طول ابتدایی بار. یک طول ابتدایی بار باید کوتاهتر از طول ابتدایی بارهای پشتیبانی شده، بزرگتر یا مساوی صفر بایت باشند. طول ابتدایی بار دیگر باید بزرگتر از طول ابتدایی بار پشتیبانی شده، کوچکتر یا مساوی ۳۲ بایت (۲۵۶ بیت) باشند.
- دو یا سه طول داده مرتبط. یک طول داده مرتبط در صورت پشتیبانی باید صفر باشد. یکی از طول‌های داده مرتبط باید کوتاهتر از طول ابتدایی بار پشتیبانی شده، بزرگتر یا مساوی صفر بایت باشد. طول یکی از داده‌های مرتبط باید بزرگتر از طول ابتدایی بار پشتیبانی شده، کوچکتر یا مساوی ۳۲ بایت (۲۵۶ بیت) باشد. اگر پیاده‌سازی از طول داده ۲۱۶ بایت پشتیبانی کند باید طول داده مرتبط ۲۱۶ بایتی آزموده شود.
- طول‌های مقطعی. همه طول‌های مقطعی شامل طول‌های بین ۷ و ۱۳ بایت، باید آزموده شوند.
- طول‌های برچسب. همه طول‌های برچسب پشتیبانی شده ۴، ۶، ۸، ۱۰، ۱۲ و ۱۳ بایتی باید آزمایش شوند.

برای آزمون قابلیت کارکردی تولید رمزگذاری AES-CCM ارزیاب چهار آزمون زیر را انجام خواهد داد:

- **آزمون ۱**: برای **هر** (EACH) کلید پشتیبانی شده و طول داده مرتبط و **هر** (ANY) ابتدایی بار پشتیبانی شده، طول برچسب و مقطعی، ارزیاب یک مقدار کلید، یک مقدار مقطعی و ۱۰ زوج داده مرتبط و مقادیر ابتدایی بار را توزیع خواهد کرد و متن رمز حاصل را کسب خواهد نمود.

- **آزمون ۲**: برای **هر** (EACH) کلید پشتیبانی شده، طول ابتدایی بار و **هر** (ANY) داده مرتبط پشتیبانی شده، طول مقطعی و برچسب، ارزیاب یک مقدار کلید، یک مقدار مقطعی و ۱۰ زوج داده مرتبط را توزیع خواهد کرد و متن رمز حاصل را کسب خواهد نمود.
- **آزمون ۳**: : برای **هر** (EACH) کلید پشتیبانی شده، طول مقطعی و **هر** (ANY) داده مرتبط پشتیبانی شده، طول برچسب و ابتدایی بار، ارزیاب یک مقدار کلید و ۱۰ زوج داده مرتبط و مقدار ابتدایی بار مقدار مقطعی سه تایی را توزیع خواهد کرد و متن رمز حاصل را کسب خواهد نمود.
- **آزمون ۴**: برای **هر** (EACH) کلید پشتیبانی شده، طول برچسب و **هر** (ANY) داده‌های مرتبط پشتیبانی شده، طول مقطعی و برچسب، ارزیاب یک مقدار کلید، یک مقدار مقطعی و ۱۰ زوج داده مرتبط و مقادیر ابتدایی بار را توزیع خواهد کرد و متن رمز حاصل را کسب خواهد نمود.

برای تعیین درستی هر یک از آزمون‌های فوق، ارزیاب متن رمز را با نتیجه تولید رمزگذاری همان ورودی‌ها با یک پیاده‌سازی خوب معلوم مقایسه خواهد نمود.

برای آزمودن قابلیت کارکردی درستی سنجی رمزگشائی AES-CCM برای **هر** (EACH) ترکیب از طول داده مرتبط پشتیبانی شده، طول ابتدایی بار، طول مقطعی و طول برچسب، ارزیاب باید یک مقدار کلید و ۱۵ طول مقطعی، داده مرتبط و متن رمز سه تایی توزیع کند و برای هر کدام یک نتیجه **رد** یا یک نتیجه **قبول** با ابتدایی بار رمزگشائی شده بدست آورد. ارزیاب به ازای هر مجموعه ۱۵ تائی ۱۰ تائی‌هایی را که بهتر است **رد** و ۵ تایی‌هایی را که بهتر است **قبول** شوند تأمین خواهد کرد.

علاوه بر این، ارزیاب از آزمون‌هایی از سند IEEE 802.1102/362r6 "بردارهای اولیه پیشنهادی برای IEEE 802.11 TGi " مورخ ۱۰ سپتامبر ۲۰۰۲، بخش ۲,۱ مثال کپسوله‌سازی AES-CCMP و بخش ۲,۲ بردارهای آزمون افزوده AES-CCMP برای بررسی بیشتر پیاده‌سازی AES-CCMP از IEEE 802.11-2007 استفاده خواهد کرد.

آزمون AES-GCM

ارزیاب قابلیت کارکردی رمزگذاری احراز اصالت شده AES-GCM را برای هر ترکیبی از طول پارامترهای ورودی زیر آزمایش خواهد کرد:

- کلید های ۱۲۸ بیتی و ۲۵۶ بیتی
- دو طول متن خام. یک طول متن خام باید در صورت پشتیبانی عدد صحیح غیر صفر مضربی از ۱۲۸ بیت باشد. طول متن خام دیگر در صورت پشتیبانی نباید عدد صحیح مضربی از ۱۲۸ بیت باشد.
- سه طول AAD. یک طول AAD باید در صورت پشتیبانی صفر باشد. یک طول AAD در صورت پشتیبانی باید عدد صحیح غیر صفری مضرب ۱۲۸ بیت باشد. یک طول AAD در صورت پشتیبانی نباید عدد صحیح غیر صفری مضرب ۱۲۸ بیت باشد.
- دو طول بردار اولیه. اگر بردار اولیه ۹۶ بیتی پشتیبانی شود، باید یکی از دو طول بردار اولیه تست شده ۹۶ بیت باشد.

ارزیاب قابلیت کارکردی رمزگذاری را با استفاده از مجموعه‌ای از ۱۰ کلید، متن خام، AAD، و بردار اولیه چندتایی برای هر ترکیب طول پارامتر بالا خواهد آزمود و مقدار متن رمز و برچسبی که از رمزگذاری احراز اصالت شده AES-GCM حاصل می‌شود را به دست خواهد آورد. هر طول برچسب پشتیبانی شده باید حداقل به ازای هر ۱۰ مجموعه یکبار آزموده شوند. مقدار بردار اولیه ممکن است توسط ارزیاب یا پیاده‌سازی آزموده شده معلومی تأمین شود.

ارزیاب قابلیت کارکردی رمزگشائی را با استفاده از یک مجموعه از ۱۰ کلید، متن رمز، برچسب، AAD، و بردار اولیه پنج تایی برای هر ترکیبی از طول پارامترهای بالا آزمایش خواهد کرد و نتیجه قبول یا رد از احراز هویت و متن خام رمزگشائی شده‌ای که پذیرفته شده باشد بدست می‌آورد. این مجموعه شامل ۵ تائی است که رد شده است و ۵ تائی که پذیرفته شده است.

نتایج حاصل از هر آزمونی ممکن است مستقیماً توسط ارزیاب و یا با تأمین ورودی در مجری و دریافت نتایج در پاسخ به دست آید. برای تعیین درستی، ارزیاب مقادیر نتیجه را با آن‌هایی که با ارسال همان ورودی‌ها در یک پیاده‌سازی خوب معلوم به دست آمده است مقایسه می‌کند.

آزمون XTS-AES

ارزیاب قابلیت کارکردی XTS-AES را برای هر ترکیبی از طول‌های پارامتر ورودی زیر مقایسه خواهد کرد:

- کلید های ۲۵۶ بیتی (برای AES-128) و ۵۱۲ بیتی (برای AES-256)
- سه طول یکای داده‌ای[۷۴] (به طور مثال، متن خام). یکی از طول‌های یکای داده‌ای در صورت پشتیبانی، باید یک عدد صحیح غیر صفر مضربی از ۱۲۸ بیت باشد. یکی از طول‌های یکای داده‌ای باید در صورت پشتیبانی، عدد صحیحی مضرب ۱۲۸ بیت باشد. طول یکای داده‌ای سوم باید یا بزرگتر از طول یکای داده پشتیبانی شده یا ۲۱۶ بیت باشد، هر کدام که کوچکتر است.
- با استفاده از مجموعه‌ای از ۱۰۰سه تایی (کلید، متن خام، مقدار تنظیمی تصادفی ۱۲۸ بیتی) و کسب متن رمزی که از رمزگذاری XTS-AES حاصل می‌شود.

ارزیاب ممکن است در صورتی که پیاده‌سازی پشتیبانی کند، به جای مقدار تنظیمی عدد متوالی یکای داده‌ای را توزیع کند. عدد متوالی یکای داده‌ای یک عدد مبنای ۱۰ است که در طیف ۰ تا ۲۵۵ قرار دارد که پیاده‌سازی‌ها را به صورت داخلی به مقدار تنظیمی تبدیل می‌کنند.

ارزیاب قابلیت کارکردی رمزگشایی XTS-AES را با استفاده از همان آزمونی که برای رمزگذاری است و با جایگذاری مقادیر متن خام با مقادیر متن رمز و رمزگذاری XTS-AES با رمز گشائی XTS-AES انجام خواهد داد.

آزمون پوشاندن کلید در استاندارد رمزگذاری پیشرفته (AES-KW) و پوشاندن کلید با لایه‌گذاری در استاندارد رمزگذاری پیشرفته (AES-KWP)

ارزیاب قابلیت کارکردی رمزگذاری احراز اصالت شده پوشاندن کلید استاندارد رمزگذاری پیشرفته را برای **هر** (EACH) ترکیبی از طول پارامترهای ورودی زیر آزمایش خواهد کرد:

[۷۴] data unit lengths

- کلیدهای رمزگذاری کلید ۱۲۸ و ۲۵۶ بیتی (KEK[۷۵])
- سه طول متن خام. یکی از طول‌های متن خام باید دو نیم قالب (۱۲۸ بیت) باشند. یکی از طول‌های متن رمز باید سه نیم قالب (۱۹۲ بیت) باشند. طول یکای داده سوم باید بزرگتر از طول متن خام پشتیبانی شده، کوچکتر یا مساوی شصت و چهار نیم قالب (۴۰۹۶ بیت) باشد.

با استفاده از مجموعه‌ای از ۱۰۰ زوج کلید و متن خام و به دست آوردن متن رمز حاصل از رمزگذاری احراز اصالت شده پوشاندن کلید استاندارد رمزگذاری پیشرفته، ارزیاب برای تعیین درستی، از تابع رمزگذاری احراز اصالت شده پوشاندن کلید استاندارد رمزگذاری پیشرفته از یک پیاده‌سازی خوب معلوم استفاده خواهد نمود.

ارزیاب قابلیت کارکردی رمزگشایی احراز اصالت شده پوشاندن کلید استاندارد رمزگذاری پیشرفته را با استفاده از همان آزمونی که برای رمزگذاری احراز اصالت شده است و با جایگذاری مقادیر متن خام با مقادیر متن رمز و رمزگذاری احراز اصالت شده پوشاندن کلید استاندارد رمزگذاری پیشرفته با رمز گشائی احراز اصالت شده پوشاندن کلید استاندارد رمزگذاری پیشرفته انجام خواهد داد.

ارزیاب قابلیت کارکردی رمزگذاری احراز اصالت شده پوشاندن کلید با لایه‌گذاری استاندارد رمزگذاری پیشرفته را با استفاده از همان آزمون رمزگذاری احراز اصالت شده پوشاندن کلید استاندارد رمزگذاری پیشرفته با تغییرات زیر در سه طول متن خام خواهد آزمود:

- یک طول متن خام باید یک هشتایی باشد. یک طول متن خام باید ۲۰ هشتایی (۱۶۰ بیت) باشد.
- یک طول متن خام باید بزرگتر از طول متن خام پشتیبانی شده و کوچکتر یا مساوی ۵۱۲ هشتایی (۴۰۹۶ بیت) باشد.

[۷۵] key encryption key

ارزیاب قابلیت کارکردی رمزگشایی احراز اصالت شده پوشاندن کلید با لایه‌گذاری استاندارد رمزگذاری پیشرفته را با استفاده از همان آزمونی که برای رمزگذاری احراز اصالت شده پوشاندن کلید استاندارد با لایه‌گذاری رمزگذاری پیشرفته است و با جایگذاری مقادیر متن خام با مقادیر متن رمز و رمزگذاری احراز اصالت شده پوشاندن کلید با لایه‌گذاری استاندارد رمزگذاری پیشرفته با رمز گشائی احراز اصالت شده پوشاندن کلید با لایه‌گذاری استاندارد رمزگذاری پیشرفته انجام خواهد داد.

۸-۵ اقدامات تضمین الزام کارکرد امنیتی عملیات رمزنگاری – چکیده‌سازی ((FCS_COP.1.1(2)

ارزیاب ارتباط تابع چکیده‌ساز را با دیگر توابع رمزنگاری برنامه‌کاربردی (برای مثال، تابع درستی‌سنجی امضای دیجیتال) که در خلاصه مشخصه محصول مستند شده است بررسی خواهد کرد.

تابع چکیده‌سازی توابع هدف امنیتی، می‌تواند در یکی از دو مد زیر پیاده‌سازی شود. مد اول مد بایت-محور است. در این مد توابع هدف امنیتی تنها پیام‌هایی را چکیده‌سازی خواهد کرد که طولشان عدد صحیحی از بایت‌ها باشد. به طور مثال طول پیامی که چکیده‌سازی خواهد شد (از نظر بیت) بر ۸ تقسیم پذیر است. مد دوم مد بیت-محور است. در این مد توابع هدف امنیتی پیام‌هایی با طول اختیاری را چکیده‌سازی خواهد کرد. از آنجا که برای هر مد آزمون‌های مختلفی وجود دارد، در بخش‌های پیش رو برای آزمون‌های MAC بیت محور در مقابل بایت محور نشانه‌ای داده شده است. ارزیاب همه آزمون‌های زیر را برای هر الگوریتم چکیده‌سازی پیاده‌سازی شده توسط توابع هدف امنیتی و مورد استفاده برای برآوردن الزامات این پروفایل حفاظتی انجام خواهد داد.

آزمون‌های زیر مستلزم این است که توسعه‌دهنده دسترسی به یک برنامه‌کاربردی آزمون را فراهم آورد که ابزاری را به ارزیاب ارائه می‌دهد که به طور معمول در برنامه‌کاربردی تولید شده یافت نمی‌شوند.

- **آزمون ۱**: آزمون پیام‌های کوتاه (مد بیت محور)- ارزیاب مجموعه ورودی‌ای شامل m+1 پیام را که در آن m طول قالب الگوریتم چکیده‌ساز است تولید می‌کند. طول پیام‌ها به طور متوالی طیفی از صفر تا m بیت را تشکیل می‌دهند. متن پیام باید به طور شبه تصادفی ایجاد شده باشد. ارزیاب خلاصه پیام را برای هر پیام محاسبه خواهد کرد و اطمینان حاصل می‌کند که نتایج درستی از پیام‌های ارائه شده به توابع هدف امنیتی تولید شده است.
- **آزمون ۲**: آزمون پیام‌های کوتاه (مد بایت محور)- ارزیاب مجموعه ورودی‌ای شامل m/8+1 پیام را که در آن m طول قالب الگوریتم چکیده‌ساز است تولید می‌کند. طول پیام‌ها به طور متوالی طیفی از صفر تا m/8 بایت را تشکیل می‌دهند که هر متن عدد صحیحی از بایت‌ها می‌باشد. متن پیام باید به طور شبه تصادفی ایجاد شده باشد. ارزیاب خلاصه پیام را برای هر پیام محاسبه خواهد کرد و اطمینان حاصل می‌کند که نتایج درستی از پیام‌های ارائه شده به توابع هدف امنیتی تولید شده است.
- **آزمون ۳**: آزمون پیام‌ها با طول انتخابی (مد بیت محور)- ارزیاب مجموعه ورودی‌ای شامل m پیام را که در آن m طول قالب الگوریتم چکیده‌ساز است تولید می‌کند. طول پیام‌ها 512+99.i که $1 < i \leq m$ می‌باشد. متن پیام باید به طور شبه تصادفی ایجاد شده باشد. ارزیاب خلاصه پیام را برای هر پیام محاسبه خواهد کرد و اطمینان حاصل می‌کند که نتایج درستی از پیام‌های ارائه شده به توابع هدف امنیتی تولید شده است.
- **آزمون ۴**: آزمون پیام‌ها با طول انتخابی (مد بایت محور)- ارزیاب مجموعه ورودی‌ای شامل m/8 پیام را که در آن m طول قالب الگوریتم چکیده‌ساز است تولید می‌کند. طول پیام‌ها 512+8.99.i که $1 < i \leq m/8$ می‌باشد. متن پیام باید به طور شبه تصادفی ایجاد شده باشد. ارزیاب خلاصه پیام را برای هر پیام محاسبه خواهد کرد و اطمینان حاصل می‌کند که نتایج درستی از پیام‌های ارائه شده به توابع هدف امنیتی تولید شده است.
- **آزمون ۵**: آزمون پیام‌های شبه تصادفی تولید شده – این آزمون تنها برای پیاده‌سازی‌های بایت محور است. ارزیاب به صورت تصادفی نقطه آغازی ایجاد می‌کند که طول آن n بیت باشد، که در آن n طول پیام چکیده تولید شده با تابع چکیده‌سازی است که باید مورد آزمون قرار گیرد. ارزیاب مجموعه‌ای از ۱۰۰ پیام و چکیده‌های

مربوطه را با پیروی از الگوریتم ارائه شده در شکل ۱ [SHAVS] فرموله خواهد کرد. ارزیاب سپس اطمینان حاصل خواهد کرد که هنگامی که پیام‌ها به توابع هدف امنیتی ارائه شده‌اند نتایج درستی تولید شده‌اند.

۸-۶ اقدامات تضمین الزام کارکرد امنیتی عملیات رمزنگاری – امضا کردن (FCS_COP.1(3))

ارزیاب اقدامات زیر را بر اساس انتخاب‌های موجود در هدف امنیتی انجام خواهد داد.

آزمون‌های زیر مستلزم این است که توسعه‌دهنده دسترسی به یک برنامه‌کاربردی آزمون را فراهم آورد، که ابزاری را برای ارزیاب ارائه می‌دهد که به طور معمول در برنامه‌کاربردی تولید شده یافت نمی‌شوند.

آزمون‌های الگوریتم ECDSA

- **آزمون ۱**: آزمون تولید امضای ECDSA FIPS 186-4. برای هر خم NIST پشتیبانی شده (به طور مثال P-256، P-384 و P-521) و زوج تابع الگوریتم چکیده‌ساز امن، ارزیاب مجموعه‌ای از ۱۰ پیام با طول ۱۰۲۴ بیت را تولید کرده و برای هر پیام یک کلید عمومی و مقادیر R و S امضای حاصل را به دست می‌آورد. برای تعیین درستی، ارزیاب از تابع درستی‌سنجی امضا از یک پیاده‌سازی خوب معلوم استفاده خواهد کرد.
- **آزمون ۲**: آزمون درستی‌سنجی امضای ECDSA FIPS 186-4. برای هر خم NIST پشتیبانی شده (به طور مثال P-256، P-384 و P-521) و زوج تابع الگوریتم چکیده‌ساز امن، ارزیاب مجموعه‌ای از ۱۰ پیام ۱۰۲۴ بیتی، کلید عمومی و امضای چندتایی تولید خواهد کرد و یکی از مقادیر (پیام، کلید عمومی یا امضاء) را در پنج تا از ۱۰ تا تغییر خواهد داد. ارزیاب تأیید می‌کند که ۵ پاسخ موفقیت و ۵ پاسخ شکست را نشان دهد.

آزمون‌های الگوریتم امضای RSA

- **آزمون ۱**: آزمون تولید امضا. ارزیاب پیاده‌سازی تولید امضای RSA توسط سیستم‌عامل را با استفاده از آزمون تولید امضا بررسی خواهد کرد. برای اجرای این آزمون ارزیاب بایستی ۱۰ پیام را از پیاده‌سازی مرجع قابل اعتماد برای ترکیب الگوریتم چکیده‌ساز امن یا اندازه واحد پشتیبانی شده توسط توابع هدف امنیتی تولید کند و یا به دست آورد. ارزیاب سیستم‌عاملی خواهد داشت که از کلید خصوصی‌اش و مقادیر واحد برای امضای این پیام‌ها استفاده می‌کند. ارزیاب درستی امضای توابع هدف امنیتی را با استفاده از یک پیاده‌سازی خوب معلوم و کلیدهای عمومی مرتبط برای تأیید امضا بررسی خواهد کرد.
- **آزمون ۲**: آزمون درستی‌سنجی امضا. ارزیاب آزمون درست‌سنجی امضا را به منظور بررسی توانایی سیستم‌عامل در تشخیص امضاهای معتبر و نامعتبر طرف‌های دیگر انجام خواهد داد. ارزیاب خطاهای بردارهای آزمون تولید شده در طول آزمون درستی‌سنجی امضا را با نشان دادن خطاها در برخی از کلیدهای عمومی، e، پیام‌ها، قالب IR، و یا امضاها تزریق خواهد کرد. ارزیاب بررسی خواهد کرد که سیستم‌عامل خرابی‌ها را هنگام اعتباردهی به هر امضا بر می‌گرداند.

۸-۷ اقدامات تضمین الزام کارکرد امنیتی عملیات رمزنگاری – احراز هویت پیام چکیده کلیددار ((4) FCS_COP.1.1)

ارزیاب اقدامات زیر را بر اساس انتخاب‌های موجود در هدف امنیتی انجام خواهد داد.

برای هر مجموعه از پارامترهای پشتیبانی شده، ارزیاب ۱۵ مجموعه از داده آزمون را تشکیل خواهد داد. هر مجموعه باید شامل یک کلید و داده پیام باشد. ارزیاب سیستم‌عاملی خواهد داشت که برچسب کد احراز هویت پیام مبتنی بر چکیده‌ساز را برای این مجموعه از داده‌های آزمون تولید می‌کند. برچسب‌های MAC حاصل باید با نتایج تولید شده از برچسب‌های کد احراز هویت پیام مبتنی بر چکیده‌ساز با همان کلید و بردار اولیه مورد استفاده توسط یک پیاده‌سازی خوب معلوم مقایسه گردد.

۸-۸ اقدامات تضمین الزام کارکرد امنیتی تولید بیت تصادفی ۱ (FCS_RBG_EXT.1.1)

ارزیاب آزمون‌های زیر را بسته به استانداردی که تولید کننده بیت تصادفی از آن تبعیت می‌کند انجام خواهد داد.

پیاده‌سازی‌هایی منطبق بر پیوست FIPS 140-2 C.

مرجع آزمون‌های گنجانده شده در این بخش سامانه اعتبارسنجی تولید کننده عدد تصادفی (RNGVS[۷۶]) است. ارزیاب دو آزمون زیر را انجام خواهد داد. توجه داشته باشید که "مقادیر مورد انتظار" با پیاده‌سازی مرجع الگوریتمی تولید شده است که دقت آن شناخته شده است. اثبات درستی برای هر طرحی گذاشته شده است.

- **آزمون ۱**: ارزیاب آزمون نقطه آغاز متغیر را انجام خواهد داد. ارزیاب مجموعه‌ای از ۱۲۸ زوج (نقطه آغاز، DT) را برای تابع تولید کننده بیت تصادفی توابع هدف امنیتی فراهم خواهد آورد که هر کدام ۱۲۸ بیت دارد. ارزیاب همچنین کلیدی (با طول مناسب برای الگوریتم استاندارد رمزنگاری پیشرفته) فراهم خواهد آورد که برای همه ۱۲۸ زوج (نقطه آغاز، DT) ثابت است. مقدار DT برای هر مجموعه‌ای ۱ افزایش خواهد داشت. مقادیر نقطه آغاز باید در مجموعه بدون تکرار باشد. ارزیاب اطمینان حاصل خواهد کرد که مقادیر برگشت داده شده توسط توابع هدف امنیتی با مقادیر مورد انتظار مطابقت دارد.
- **آزمون ۲**: ارزیاب آزمون مونت کارلو را انجام خواهد داد. برای این آزمون، نقطه آغاز ابتدایی و مقدار DT به تابع تولید کننده بیت تصادفی توابع هدف امنیتی تأمین می‌شود که هر کدام از آن‌ها ۱۲۸ بیت دارد. ارزیاب همچنین کلیدی (با طول مناسب برای الگوریتم استاندارد رمزنگاری پیشرفته) که در طول آزمون ثابت است ارائه خواهد داد. ارزیاب سپس تولید کننده بیت تصادفی توابع هدف امنیتی را ۱۰،۰۰۰ بار فراخوانی می‌کند در حالی که مقدار DT در هر تغییر به میزان ۱ واحد افزایش خواهد یافت، و نقطه آغاز جدید برای تکرار بعدی به گونه‌ای تولید می‌شود که در پیوست ANSI X9.31 A.2.4 "تولید کننده عدد تصادفی توصیه شده NIST با استفاده از سه کلید سه‌گانه DES و الگوریتم‌های استاندارد رمزنگاری پیشرفته، بخش ۳" مشخص شده است. ارزیاب اطمینان حاصل می‌کند که ۱۰،۰۰۰ اُمین مقدار تولید شده با مقدار مورد انتظار مطابقت دارد.

پیاده‌سازی‌های منطبق بر انتشارات ویژه NIST: 800-90A

[۷۶] Random Number Generator Validation System

- **آزمون ۱**: ارزیاب ۱۵ آزمایش برای پیاده‌سازی تولید کننده عدد تصادفی (RNG[۷۷]) انجام خواهد داد. اگر تولید کننده عدد تصادفی قابل پیکربندی باشد، ارزیاب ۱۵ آزمایش را برای هر پیکربندی انجام خواهد داد. ارزیاب همچنین تصدیق خواهد کرد راهنماهای عملیاتی شامل دستورالعمل‌های مناسب برای پیکربندی قابلیت کارکردی تولید کننده عدد تصادفی می‌باشد.

چنانچه تولید کننده عدد تصادفی مقاومت در برابر پیش‌بینی را فعال کرده باشد، هر آزمایش شامل این موارد خواهد بود: (۱) نمونه‌سازی تولید کننده بیت تصادفی قطعی, (۲) تولید اولین قالب از بیت‌های تصادفی (۳) تولید دومین قالب از بیت‌های تصادفی (۴) عدم نمونه‌سازی. ارزیاب تأیید می‌کند که دومین قالب از بیت‌های تصادفی مقدار مورد انتظار است. ارزیاب هشت مقدار ورودی را برای هر آزمایش تولید خواهد کرد. اولین آن شماره‌ای (۰-۱۴) است. سه تای بعدی ورودی آنتروپی، مقدار مقطعی و رشته شخصی شده برای عملیات نمونه‌سازی می‌باشد. دو تای بعدی ورودی افزوده و ورودی آنتروپی برای اولین فراخوانی تولید است. دوتای آخری ورودی افزوده و ورودی آنتروپی برای دومین فراخوانی تولید است. این مقادیر به صورت تصادفی تولید شده‌اند. "تولید یک قالب از بیت‌های تصادفی" به معنای تولید بیت‌های تصادفی با تعداد بیت برگشت داده شده مساوی با طول قالب خروجی است (همانگونه که در NIST SP 800-90A تعریف شده است).

اگر تولید کننده عدد تصادفی مقاومت در برابر پیش‌بینی را نداشت، هر آزمایش شامل این موارد خواهد بود: (۱) نمونه‌سازی تولید کننده بیت تصادفی قطعی (۲) تولید اولین قالب از بیت‌های تصادفی (۳) تولید مجدد نقطه آغاز تصادفی (۴) تولید دومین قالب از بیت‌های تصادفی (۵) عدم نمونه‌سازی. ارزیاب تأیید می‌کند که دومین قالب از بیت‌های تصادفی مقدار مورد انتظار است. ارزیاب هشت مقدار ورودی را برای هر آزمایش تولید خواهد کرد. اولین آن شماره‌ای (۰-۱۴) است. سه تای بعدی ورودی آنتروپی، مقدار مقطعی و رشته شخصی شده برای عملیات نمونه‌سازی می‌باشد. مقدار پنجم ورودی افزوده برای اولین فراخوانی تولید است. مقدار ششم و هفتم ورودی افزوده و ورودی آنتروپی برای فراخوانی تولید مجدد نقطه آغاز تصادفی است. آخرین مقدار ورودی افزوده برای دومین صدا زدن برای تولید است.

---

[۷۷] Random Number Generator

پارگراف‌های زیر حاوی اطلاعات بیشتر در مورد برخی از مقادیر ورودی که باید توسط ارزیاب تولید و یا انتخاب شوند می‌باشد.

ورودی آنتروپی: طول مقدار ورودی آنتروپی باید برابر با طول نقطه آغاز باشد.

مقدار مقطعی: اگر مقادیر مقطعی پشتیبانی شود (CTR_DRBG بدون تابع استخراج از مقدار مقطعی استفاده نخواهد کرد)، طول مقطعی نیمی از طول نقطه آغاز است.

رشته شخصی‌سازی شده: طول رشته شخصی‌سازی شده باید کمتر یا مساوی طول نقطه آغاز باشد. اگر پیاده‌سازی تنها یک طول رشته شخصی‌سازی شده را پشتیبانی کند، همان طول می‌تواند برای دو مقدار استفاده شود. اگر بیش از یک طول رشته پشتیبانی شود، ارزیاب از رشته‌های شخصی‌سازی شده با دو طول متفاوت استفاده خواهد کرد. اگر پیاده‌سازی استفاده از یک رشته شخصی‌سازی شده را پشتیبانی نکرد، نیازی نیست مقداری تأمین شود.

ورودی افزوده: طول بیت‌های ورودی افزوده همان محدودیت‌های و پیش فرض‌هایی را دارد که طول رشته‌های شخصی‌سازی شده.

۸-۹ اقدامات تضمین الزام کارکرد امنیتی تولید بیت تصادفی ۲ (FCS_RBG_EXT.1.2)

مستندات باید تولید شوند – و ارزیاب اقدامات را مطابق با موارد زیر انجام خواهد داد:

پیوست ه و تصریح پیوست مستند سازی آنتروپی و ارزیابی.

در آینده، آزمون آماری مشخص (در راستای NIST SP 800-90B) به منظور بررسی برآوردهای آنتروپی مورد نیاز خواهد بود.

۸-۱۰ اقدامات تضمین الزام کارکرد امنیتی انبارش داده حساس ۱ (FCS_STO_EXT.1.1)

ارزیاب به منظور اطمینان از اینکه خلاصه مشخصه محصول همه داده حساس پایا را فهرست می‌کند که سیستم‌عامل قابلیت کارکردی انبارش آن را ارائه داده است این خلاصه را بررسی می‌کند. ارزیاب تأیید خواهد کرد که در خلاصه مشخصه محصول برای هر یک از این آیتم‌ها این موارد فهرست شده است که هر آیتم به چه منظوری می‌تواند مورد استفاده قرار بگیرد و چگونه ذخیره شده است. ارزیاب تصدیق می‌کند که عملیات رمزنگاری مورد استفاده برای حفاظت از داده‌ها همانگونه اتفاق می‌افتد که در FCS_COP.1(1) مشخص شده است.

ارزیاب همچنین برای بررسی این موضوع که واسطی برای برنامه‌های کاربردی به منظور ذخیره امن اعتبارنامه‌ها وجود دارد با توسعه دهنده مستندات همفکری خواهد کرد.

۱۱-۸ اقدامات تضمین الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS ۱ (FCS_TLSC_EXT.1.1)

ارزیاب شرح پیاده‌سازی این پروتکل را در خلاصه مشخصه محصول بررسی خواهد کرد تا اطمینان حاصل کند که این مجموعه رمزهای پشتیبانی شده مشخص شده‌اند. ارزیاب خلاصه مشخصه محصول را بررسی می‌کند تا اطمینان یابد که مجموعه رمزهای مشخص شده شامل آن‌هایی است که در این مؤلفه فهرست شده‌اند. ارزیاب همچنین راهنمایی‌های عملیاتی را بررسی خواهد کرد تا اطمینان حاصل کند که راهنمایی‌هایی درباره پیکربندی سیستم‌عامل را در بر می‌گیرد که TLS منطبق بر توضیحاتی باشد که در خلاصه مشخصه محصول است. ارزیاب همچنین آزمون‌های زیر را انجام خواهد داد:

- **آزمون ۱**: ارزیاب یک اتصال TLS را با استفاده از هر مجموعه رمز مشخص شده توسط الزام برقرار خواهد کرد. این اتصال ممکن است به عنوان قسمتی از برقراری یک پروتکل سطح بالاتر برقرار شود به طور مثال به عنوان قسمتی از نشست پروتکل احراز هویت قابل توسعه (EAP[۷۸]). مشاهده مراوده موفقیت‌آمیز مجموعه رمز برای برآوردن هدف آزمون کافی است؛ لازم نیست در تلاش برای تشخیص این موضوع که مجموعه رمزها مورد استفاده قرار گرفته‌اند مشخصات ترافیک رمزگذاری شده مورد آزمایش قرار بگیرند (به عنوان مثال، این موضوع که الگوریتم رمزنگاری AES ۱۲۸ بیتی است و نه AES ۲۵۶ بیتی).

[۷۸] Extensible Authentication Protocol

- **آزمون ۲**: ارزیاب تلاش خواهد کرد تا اتصال را با استفاده از یک سرور با گواهی سروری برقرار کند که شامل احراز هویت سرور در رشته کاربری کلید توسعه داده شده است و تأیید کند که اتصال برقرار شده است. ارزیاب سپس بررسی خواهد کرد که سرویس‌گیرنده گواهی سرور معتبر دیگری که فاقد هدف احراز هویت سرور در رشته کاربری کلید توسعه یافته است را رد می‌کند و اتصال برقرار نمی‌شود. در حالت مطلوب هر دو گواهی باید یکسان باشند به جز در رشته کاربری کلید توسعه یافته.
- **آزمون ۳**: ارزیاب گواهی سرور در اتصال TLS را که با مجموعه رمز انتخاب شده سرور انطباق ندارد ارسال می‌کند (به عنوان مثال، یک گواهی ECDSA را هنگام استفاده از مجموعه رمز TLS_RSA_WITH_AES_128_CBC_SHA می‌فرستد یا گواهی RSA را هنگام استفاده از یکی از مجموعه رمزهای ECDSA می‌فرستد.) ارزیاب بررسی خواهد کرد که سیستم‌عامل بعد از دریافت پیام دست داد گواهی سرور اتصال را قطع می‌کند.
- **آزمون ۴**: ارزیاب سرور را برای انتخاب مجموعه رمز TLS_NULL_WITH_NULL_NULL پیکربندی خواهد کرد و بررسی می‌کند که سرویس‌گیرنده اتصال را رد می‌کند.
- **آزمون ۵**: ارزیاب تغییرات زیر را در ترافیک اعمال خواهد کرد:
  - **آزمون ۵,۱**: نسخه TLS انتخاب شده توسط سرور در سلام سرور را به یک نسخه TLS پشتیبانی نشده تغییر می‌دهد (برای مثال ۱,۳ ارائه شده توسط دو بایت ۰۳ ۰۴) و بررسی می‌کند که سرویس‌گیرنده اتصال را رد کند.
  - **آزمون ۵,۲**: حداقل یک بایت را در مقدار مقطعی سرور در پیام دست داد سلام سرور تغییر می‌دهد و بررسی می‌کند که سرویس‌گیرنده پیام دست داد تبادل کلید سرور را رد می‌کند (اگر از مجموعه رمز DHE یا ECDHE استفاده کند) یا اینکه سرور پیام دست داد پایانی سرویس‌گیرنده را رد می‌کند.

- **آزمون ۵,۳**: مجموعه رمز انتخاب شده سرور در پیام دست داد سلام سرور را به یک مجموعه رمز ارائه نشده در پیام دست داد سلام سرویس‌گیرنده تغییر می‌دهد. ارزیاب بررسی خواهد کرد که سرویس‌گیرنده بعد از دریافت سلام سرور اتصال را رد کند.
- **آزمون ۵,۴:** قالب امضا را در پیام دست داد تبادل کلید سرور تغییر می‌دهد و بررسی می‌کند که سرویس‌گیرنده بعد از دریافت پیام تبادل کلید سرور اتصال را رد کند.
- **آزمون ۵,۵:** یک بایت را در پیام دست داد پایانی سرور تغییر می‌دهد و بررسی می‌کند که سرویس‌گیرنده هشدار جدی را پس از دریافت ارسال کرده و هیچ داده‌ای از برنامه‌کاربردی ارسال نکند.
- **آزمون ۵,۶**: بعد از آن که سرور پیام تغییر تنظیمات رمز را صادر کرد، پیام نامفهومی را از سرور ارسال می‌کند و بررسی می‌کند که آیا سرویس‌گیرنده اتصال را رد می‌کند یا خیر.

۱۲-۸ اقدامات تضمین الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS ۲ (FCS_TLSC_EXT.1.2)

ارزیاب اطمینان حاصل خواهد کرد که خلاصه مشخصه محصول روش سرویس‌گیرنده را برای ایجاد همه شناسه‌های مرجع از شناسه مرجع پیکربندی شده برنامه‌کاربردی که شامل انواع شناسه‌های مرجعی است که پشتیبانی می‌شوند (به طور مثال نام‌های مشترک، نام DNS، نام URI، نام خدمت، یا دیگر نام‌های جایگزین موجودیت فعال خاص برنامه‌کاربردی) و آدرس‌های IP و کاراکترهای عمومی که پشتیبانی شده‌اند را توصیف می‌کند. ارزیاب اطمینان حاصل خواهد کرد که شناسه‌های توصیفی و روشی که پین‌گذاری گواهی پشتیبانی می‌شود پشتیبانی و یا مورد استفاده توسط سیستم‌عامل می‌باشد.

ارزیاب بررسی خواهد کرد که راهنمایی‌های سند راهنمای اجرایی شامل دستورالعمل‌هایی برای تنظیم شناسه مرجعی است که برای اهداف اعتبارسنجی گواهی در TLS استفاده می‌شوند.

ارزیاب شناسه مرجع را مطابق راهنمایی سند راهنمای اجرایی پیکربندی خواهد کرد و آزمون‌های زیر را در طول یک اتصال TLS انجام خواهد داد:

- **آزمون ۱**: ارزیاب یک گواهی سرور ارائه خواهد داد که در نام جایگزین موجودیت فعال (SAN) یا نام مشترک (CN) که با شناسه مرجع انطباق می‌یابد شناسه‌ای را در برنمی‌گیرد. ارزیاب بررسی خواهد کرد که اتصال با شکست مواجه شود.
- **آزمون ۲**: ارزیاب گواهی سروری ارائه خواهد داد که شامل یک نام مشترک است که با شناسه مرجع تطابق دارد که گسترش نام جایگزین موجودیت فعال را در برمی‌گیرد اما شناسه‌ای در نام جایگزین موجودیت فعال که با شناسه مرجع انطباق داشته باشد را شامل نمی‌شود. ارزیاب بررسی خواهد کرد که اتصال با شکست مواجه شود. ارزیاب این آزمون را برای هر نوع در نام جایگزین موجودیت فعال پشتیبانی شده تکرار خواهد کرد.
- **آزمون ۳**: ارزیاب یک گواهی سرور ارائه خواهد داد که شامل نام مشترکی است که با شناسه مرجع تطابق دارد و شامل بسط نام جایگزین موجودیت فعال نمی‌باشد. ارزیاب بررسی خواهد کرد که اتصال با موفقیت صورت گیرد.
- **آزمون ۴**: ارزیاب گواهی سروری ارائه خواهد داد که شامل نام مشترکی است که با شناسه مرجع انطباق ندارد اما شامل شناسه‌ای در نام جایگزین موجودیت فعال است که انطباق دارد. ارزیاب بررسی خواهد کرد که اتصال با موفقیت صورت گیرد.
- **آزمون ۵**: ارزیاب آزمون کاراکترهای عمومی زیر را با هر نوع شناسه مرجع پشتیبانی شده انجام خواهد داد:
  - **آزمون ۵,۱**:.ارزیاب گواهی سروری ارائه خواهد داد که شامل یک کاراکتر عمومی در سمت چپ برچسب شناسه ارائه شده نیست (به طور مثال Foo.*.example.com) و بررسی خواهد کرد که اتصال با شکست مواجه شود.

- **آزمون ۵,۲**:.ارزیاب گواهی سروری ارائه خواهد داد که شامل یک کاراکتر عمومی در سمت چپ برچسب است اما قبل از یک پسوند عمومی نیست (به طور مثال example.com.*). ارزیاب شناسه مرجع را با یک برچسب تنها در سمت چپ پیکربندی خواهد کرد (به طور مثال Foo.example.com) و بررسی خواهد کرد که اتصال با موفقیت صورت گیرد. ارزیاب شناسه مرجع را بدون برچسب سمت چپ همانگونه که در گواهی است پیکربندی خواهد کرد (به طور مثال example.com) و بررسی خواهد کرد که اتصال با شکست مواجه شود. ارزیاب شناسه مرجع را با دو برچسب سمت چپ پیکربندی خواهد کرد (به طور مثال bar.foo.example.com) و بررسی خواهد کرد که اتصال با شکست مواجه شود.
- **آزمون ۵,۳**: ارزیاب گواهی سروری ارائه خواهد داد که شامل یک کاراکتر عمومی در سمت چپ برچسب است که بلافاصله قبل از یک پسوند عمومی می‌باشد (به طور مثال com.*). ارزیاب شناسه مرجع را با یک برچسب تنها در سمت چپ پیکربندی خواهد کرد (به طور مثال Foo.com) و بررسی می‌کند که اتصال با شکست مواجه شود. ارزیاب شناسه مرجع را با دو برچسب سمت چپ پیکربندی خواهد کرد (به طور مثال bar.foo.com) و بررسی خواهد کرد که اتصال با شکست مواجه شود.
- **آزمون ۶:** [شرطی] اگر URI یا شناسه مرجع نام خدمت پشتیبانی شده باشند، ارزیاب نام DNS و شناسه خدمت را پیکربندی خواهد کرد. ازریاب گواهی سرویسی شامل نام DNS درست و شناسه سرویس در نام URI یا رشته‌های نام SRV از نام جایگزین موجودیت فعال ارائه خواهد کرد و بررسی می‌کند که اتصال با موفقیت برقرار شود. ارزیاب این آزمون را با شناسه خدمت اشتباه (اما نام DNS درست) انجام خواهد داد و بررسی خواهد کرد که اتصال با شکست مواجه شود.
- **آزمون ۷**: [شرطی] اگر گواهی‌های پین شده پشتیبانی شوند ارزیاب گواهی‌ای ارائه خواهد داد که با گواهی پین شده مطابقت ندارد و بررسی خواهد کرد که اتصال با شکست مواجه شود.

۸-۱۳ اقدامات تضمین الزام کارکرد امنیتی پروتکل سرویس‌گیرنده TLS ۳ (FCS_TLSC_EXT.1.3)

ارزیاب از TLS به عنوان تابعی برای بررسی این موضوع که قوانین اعتبار سنجی در FIA_X509_EXT.1.1 رعایت شده‌اند استفاده خواهد کرد و آزمون افزوده زیر را انجام خواهد داد:

- **آزمون ۱**: ارزیاب نشان خواهد داد که همتایی که از یک گواهی استفاده می‌کند بدون مسیر گواهی معتبر منجر به شکست در احراز اصالت می‌شود. با استفاده از راهنمایی‌های اجرایی، ارزیاب گواهی(های) CA قابل اعتمادی که برای اعتبار سنجی گواهی‌های متناظر لازم است را بارگذاری خواهد کرد، و نشان می‌دهد که اتصال با موفقیت صورت گرفته است. ارزیاب سپس باید یکی از گواهی‌های CA را پاک کند، و نشان دهد که اتصال با شکست مواجه شده است.
- **آزمون ۲**: ارزیاب نشان خواهد داد که همتایی که از گواهی استفاده می‌کند که باطل شده است منجر به شکست در اصالت‌سنجی می‌شود.
- **آزمون ۳**: ارزیاب نشان می‌دهد که همتایی که از گواهی استفاده می‌کند که تاریخ انقضای آن گذشته است، منجر به شکست در اصالت‌سنجی می‌شود.
- **آزمون ۴**: ارزیاب نشان می‌دهد که همتایی که از گواهی استفاده می‌کند که شناسه معتبری ندارد باید منجر به شکست در اصالت‌سنجی شود.

۸-۱۴ اقدامات تضمین الزام کارکرد امنیتی کنترل‌های دسترسی برای حفاظت از داده کاربر ۱ (FDP_ACF_EXT.1.1)

ارزیاب تصدیق خواهد کرد که خلاصه مشخصه محصول به طور جامع خط‌مشی کنترل دسترسی اعمال شده توسط سیستم‌عامل را شرح می‌دهد. توضیحات باید شامل قوانینی باشد که با آن دسترسی‌ها به فایل‌ها و دایرکتوری‌های خاص برای کاربران خاص مشخص شده است. ارزیاب خلاصه مشخصه محصول را مورد بازرسی قرار خواهد داد تا اطمینان حاصل کند که قوانین کنترل دسترسی با را جزئیاتی توضیح داده‌است که برای هر سناریوی داده شده ممکن، تصمیمات کنترل دسترسی بین یک کاربر و یک فایل تحت حاکمیت سیستم‌عامل بدون ابهام است.

ارزیاب دو حساب کاربری کاربر استاندارد جدید را روی سامانه ایجاد خواهد کرد و آزمون‌های زیر را انجام خواهد داد:

- **آزمون ۱**: ارزیاب به عنوان کاربر اول در سامانه احراز هویت خواهد کرد و فایلی را در دایرکتوری خانه کاربر ایجاد خواهد کرد. سپس ارزیاب از سامانه خارج شده و به عنوان کاربر دوم وارد می‌شود. ارزیاب تلاش خواهد کرد تا فایل ایجاد شده در دایرکتوری خانه کاربر اول را بخواند. ارزیاب اطمینان حاصل می‌کند که تلاش خواندن رد شده است.
- **آزمون ۲**: ارزیاب به عنوان کاربر اول در سامانه احراز هویت خواهد کرد و فایلی را در دایرکتوری خانه کاربر ایجاد خواهد کرد. سپس ارزیاب از سامانه خارج شده و به عنوان کاربر دوم وارد می‌شود. ارزیاب تلاش خواهد کرد تا در فایل ایجاد شده در دایرکتوری خانه کاربر اول تغییراتی ایجاد کند. ارزیاب اطمینان حاصل می‌کند که تغییر رد شده است.
- **آزمون ۳**: ارزیاب به عنوان کاربر اول در سامانه احراز هویت خواهد کرد و فایلی را در دایرکتوری کاربری کاربر ایجاد خواهد کرد. سپس ارزیاب از سامانه خارج شده و به عنوان کاربر دوم وارد می‌شود. ارزیاب تلاش خواهد کرد تا فایل ایجاد شده در دایرکتوری خانه کاربر اول را حذف کند. ارزیاب اطمینان حاصل می‌کند که حذف کردن رد شده است.
- **آزمون ۴**: ارزیاب به عنوان کاربر اول در سامانه احراز هویت خواهد کرد. ارزیاب تلاش خواهد کرد تا فایلی را در دایرکتوری خانه کاربر دوم ایجاد کند. ارزیاب اطمینان حاصل می‌کند که ایجاد فایل رد شده است.
- **آزمون ۵**: ارزیاب به عنوان کاربر اول در سامانه احراز هویت خواهد کرد و تلاش خواهد کرد تا در فایل ایجاد شده در دایرکتوری خانه کاربر اول تغییراتی ایجاد کند. ارزیاب اطمینان حاصل می‌کند که تغییر در فایل پذیرفته شده است.

- **آزمون ۶**: ارزیاب به عنوان کاربر اول در سامانه احراز هویت خواهد کرد و تلاش خواهد کرد تا فایل ایجاد شده در دایرکتوری خانه کاربر اول را حذف کند. ارزیاب اطمینان حاصل می‌کند که حذف فایل پذیرفته شده است.

۸-۱۵ اقدامات تضمین الزام کارکرد امنیتی کنترل جریان اطلاعات ۱ (FDP_IFC_EXT.1.1)

ارزیاب بررسی خواهد کرد که بخش خلاصه مشخصه محصول هدف امنیتی مسیریابی ترافیک IP را زمانی که سرویس‌گیرنده شبکه خصوصی مجازی فعال است توضیح می‌دهد. ارزیاب اطمینان حاصل می‌کند که توضیحات نشان می‌دهد که کدام ترافیک از طریق شبکه خصوصی مجازی عبور نمی‌کند و کدام عبور می‌کند، و همچنین اطمینان می‌یابد پیکربندی‌ای برای هر کدام وجود دارد که تنها ترافیکی که توسط نویسنده هدف امنیتی که برای برقراری اتصال شبکه خصوصی مجازی ضروری تشخیص داده شده است (ترافیک IKE و شاید HTTPS یا ترافیک DNS) توسط پروتکل شبکه خصوصی مجازی (IPsec) محصور نیست.

۸-۱۶ اقدامات تضمین الزام کارکرد امنیتی مدیریت رفتار توابع امنیتی ۱ (FMT_MOF_EXT.1.1)

ارزیاب بررسی خواهد کرد که هر تابع مدیریت اتخاذ شده در هدف امنیتی در راهنمای عملیاتی شرح داده شده است و این توضیحت شامل اطلاعات مورد نیاز برای انجام وظایف مدیریت مرتبط با توابع مدیریتی می‌باشد. ارزیاب توانایی سیستم‌عامل را در ارائه توابع مدیریتی با پیکربندی سیستم‌عامل و آزمایش هر یک از گزینه‌های انتخابی بالا خواهد آزمود. انتظار می‌رود ارزیاب این توابع را به همه روش‌هایی که در مستندات هدف امنیتی و راهنما بیان شده است که پیکربندی می‌تواند مدیریت شود آزمایش کند.

۸-۱۷ اقدامات تضمین الزام کارکرد امنیتی کنترل‌های دسترسی ۱ (FPT_ACF_EXT.1.1)

ارزیاب تأیید خواهد کرد که خلاصه مشخصه محصول موقعیت درایورها و ماژول‌های هسته، ثبت‌های وقایع ممیزی امنیتی، کتابخانه‌های مشترک، فایل‌های اجرایی سامانه، فایل‌های پیکربندی سامانه را مشخص می‌کند. نیازی نیست هر فایلی به صورت جداگانه شناسایی شود، اما قراردادهای سامانه برای انبارش و محافظت از چنین فایل‌هایی باید مشخص شود. ارزیاب یک حساب کاربری غیر ممتاز ایجاد خواهد کرد. با استفاده از این حساب، ارزیاب اطمینان حاصل خواهد کرد که آزمون‌های زیر منجر به نتایج منفی می‌شود (به طور مثال، اقدام منجر به رد مجوز ارزیاب برای انجام اقدام می‌شود):

- **آزمون ۱:** ارزیاب تلاش خواهد کرد تا همه درایورها و ماژول‌های هسته را تغییر دهد.
- **آزمون ۲:** ارزیاب تلاش خواهد کرد تا همه ثبت‌های وقایع امنیتی تولید شده توسط زیر سامانه‌های ورودی را تغییر دهد.
- **آزمون ۳:** ارزیاب تلاش خواهد کرد تا همه کتابخانه‌های مشترک مورد استفاده در سرتاسر سامانه را تغییر دهد.
- **آزمون ۴:** ارزیاب تلاش خواهد کرد تا همه فایل‌های اجرایی سامانه را تغییر دهد.
- **آزمون ۵:** ارزیاب تلاش خواهد کرد تا همه فایل‌های پیکربندی سامانه را تغییر دهد.
- **آزمون ۶:** ارزیاب تلاش خواهد کرد تا هر مؤلفه افزوده انتخاب شده را تغییر دهد.

۱۸-۸ اقدامات تضمین الزام کارکرد امنیتی کنترل‌های دسترسی ۲ (FPT_ACF_EXT.1.2)

ارزیاب حساب کاربری غیر ممتازی ایجاد خواهد کرد. با استفاده از این حساب کاربری، ارزیاب اطمینان حاصل می‌کند که آزمون‌های زیر منجر به نتایج منفی می‌شود (به طور مثال، اقدام منجر به رد مجوز ارزیاب برای انجام اقدام می‌شود):

- **آزمون ۱:** ارزیاب تلاش خواهد کرد تا همه ثبت‌های وقایع امنیتی تولید شده توسط زیر سامانه‌های ممیزی را بخواند.

- **آزمون ۲:** ارزیاب تلاش خواهد کرد تا همه مخازن اعتبار نامه گسترده در سامانه را بخواند.
- **آزمون ۳:** ارزیاب تلاش خواهد کرد تا هر مؤلفه مشخص شده در اختصاص را بخواند.

۸-۱۹ اقدامات تضمین الزام کارکرد امنیتی تصادفی‌سازی چیدمان فضای آدرس ۱ (FPT_ASLR_EXT.1.1)

ارزیاب سه فایل اجرایی گنجانده شده در توابع هدف امنیتی را انتخاب می‌کند. این‌ها باید شامل هرگونه مرورگر وب یا سرویس‌گیرنده پستی گنجانده شده در توابع هدف امنیتی باشد. برای هر یک از این برنامه‌های کاربردی، ارزیاب همان فایل‌های اجرایی را در دو نمونه جدا از سیستم‌عامل بر روی سخت‌افزارهای یکسان آغاز می‌کند و همه مکان‌های نگاشت حافظه را مقایسه می‌کند. ارزیاب اطمینان حاصل می‌کند که هیچ نگاشتی از حافظه در همان مکان قرار داده نشود. اگر این اتفاق نادر رخ دهد که دو نگاشت برای یک فایل قابل اجرای منحصر به فرد یکی هستند و برای دوتای دیگر یکی نیستند، ارزیاب آزمون را با آن فایل اجرایی تکرار خواهد کرد تا بررسی کند که در آزمون دوم نگاشت‌ها متفاوت هستند.

۸-۲۰ اقدامات تضمین الزام کارکرد امنیتی حفاظت از سرریز بافر پشته ۱ (FPT_SBOP_EXT.1.1)

ارزیاب تعیین خواهد کرد که خلاصه مشخصه محصول شامل توصیفی از محافظت‌های سرریز بافر مبتنی بر پشته مورد استفاده توسط سیستم‌عامل است. پیاده‌سازی‌های نمونه ممکن است از طریق گزینه‌های انتخابی کامپایلر مانند "-fstack-protector-all"، "-fstack-protector"، وپرچم‌های "/GS" فعال شود. این‌ها

با اصطلاحات گوناگونی مانند کوکی پشته[۷۹]، گارد پشته[۸۰]، و قناری‌های پشته[۸۱] معرفی شده‌اند. خلاصه مشخصه محصول باید منطقی را برای هر فایل باینری‌ای که به این روش محافظت نشده‌اند در برگیرد.

- **آزمون ۱:** ارزیاب فهرست کاملی از هسته، کتابخانه‌ها، و فایل‌های باینری برنامه‌کاربردی تهیه خواهد کرد تا آن‌هایی را که حفاظت سرریز بافر مبتنی بر پشته پیاده‌سازی نمی‌کنند مشخص شود. این فهرست بهتر است با فهرست ارائه شده در خلاصه مشخصه محصول مطابقت داشته باشد.

۸-۲۱ اقدامات تضمین الزام کارکرد امنیتی یکپارچگی راه‌اندازی ۱ (FPT_TST_EXT.1.1)

ارزیاب بررسی خواهد کرد که بخش خلاصه مشخصه محصول هدف امنیتی شامل توصیف جامعی از روش‌های اجرایی راه‌اندازی از جمله شرحی از تمام زنجیره راه‌اندازی برای توابع هدف امنیتی باشد. ارزیاب اطمینان حاصل خواهد کرد که سیستم‌عامل به صورت رمزنگاری تأیید می‌کند که هر بخشی از نرم‌افزار که سیستم‌عامل در زنجیره راه‌اندازی بارگذاری می‌کند شامل بار کننده راه‌انداز و هسته است. نرم‌افزار بارگذاری شده برای اجرا به طور مستقیم توسط سکو (به طور مثال بار کننده راه‌انداز مرحله اول) خارج از دامنه کاربرد است. برای هر رده‌بندی افزوده‌ای از کدهای اجرایی تأیید شده قبل از اجرا، ارزیاب بررسی خواهد کرد که توضیحات موجود در خلاصه مشخصه محصول توضیح دهد که چگونه نرم‌افزار به طور رمزنگاری شده تأییده شده است.

ارزیاب بررسی خواهد کرد که خلاصه مشخصه محصول شامل شرحی از حفاظت فراهم شده برای ساز و کارهایی است که درستی‌سنجی رمزنگاری را انجام می‌دهد.

ارزیاب آزمون‌های زیر را انجام خواهد داد:

---

[۷۹] stack cookie

[۸۰] stack guard

[۸۱] Stack canaries: are known values that are placed between a buffer and control data on the stack to monitor buffer overflows/ https://en.wikipedia.org/wiki/Buffer_overflow_protection

- **آزمون ۱:** ارزیاب اقداماتی را انجام خواهد داد که باعث می‌شود نرم‌افزار توابع هدف امنیتی بارگذاری شود و مشاهده می‌کند که ساز و کارهای یکپارچگی هیچ فایل اجرایی‌ای را به عنوان فایلی که دارای خطاهای یکپارچگی است علامت دار نکرده و سیستم‌عامل به درستی راه‌اندازی می‌شود.
- **آزمون ۲:** ارزیاب فایل اجرایی توابع هدف امنیتی که قسمتی از زنجیره راه‌اندازی تأییده شده توسط توابع هدف امنیتی است را تغییر می‌دهد (به طور مثال بار کننده راه‌انداز مرحله اول نباشد) و برای راه‌اندازی تلاش کند. ارزیاب اطمینان حاصل خواهد کرد که تخلف یکپارچگی فعال شده و سیستم‌عامل راه‌اندازی نمی‌شود (باید دقت شود چرا که تخلف یکپارچگی تعیین شده باعث خرابی در بارگذاری ماژول خواهد بود، و در حقیقت راهی برای نامعتبر کردن ساختار ماژول نیست).
- **آزمون ۳:** اگر نویسنده هدف امنیتی نشان دهد که درستی‌سنجی یکپارچگی با استفاده از کلید عمومی انجام شده است، ارزیاب بررسی می‌کند که ساز و کارهای به روز رسانی شامل اعتبارسنجی گواهی مطابق FIA_X509_EXT.1 می‌باشد. ارزیاب فایل اجرایی توابع هدف امنیتی را با یک گواهی که هدف امضای کد را در رشته کاربری کلید توسعه یافته ندارد به صورت دیجیتال امضا خواهد کرد و بررسی می‌کند که تخلف یکپارچگی فعال شده باشد. ارزیاب باید آزمون را با استفاده از گواهی که شامل هدف امضای کد می‌باشد تکرار کند و بررسی کند که درستی‌سنجی یکپارچگی با موفقیت انجام می‌شود. در حالت مطلوب، دو گواهی باید یکسان باشند به جز در رشته کاربری کلید توسعه یافته.

۸-۲۲ اقدامات تضمین الزام کارکرد امنیتی یکپارچگی نصب و به‌روزرسانی ۱ (FPT_TUD_EXT.1.1)

ارزیاب با استفاده از روش‌های اجرایی توضیح داده شده در مستندات یک به روز رسانی را بررسی می‌کند و تعیین می‌کند که سیستم‌عامل فهرستی از به روز رسانی‌های در دسترس را ارائه می‌دهد. آزمودن این قابلیت ممکن است مستلزم نصب و قرار دادن موقت سامانه در پیکربندی‌ای متضاد با راهنمای پیکربندی امن

باشد که به روز رسانی‌های خودکار را مشخص می‌کند. (ارزیاب همچنین اطمینان حاصل خواهد کرد که این پرس و جو در یک کانال قابل اعتماد به نحوی که در FTP_ITC_EXT.1 توضیح داده شده است اتفاق می‌افتد.)

۸-۲۳ اقدامات تضمین الزام کارکرد امنیتی یکپارچگی نصب و به‌روزرسانی ۲ (FPT_TUD_EXT.1.2)

برای تست‌های زیر، ارزیاب بارگیری از یک به روز رسانی را آغاز خواهد کرد و به روز رسانی‌ها را قبل از نصب می‌گیرد. بارگیری می‌تواند از وب سایت فروشنده، مخزن به روز رسانی میزبانی شده توسط شرکت، یا سامانه دیگری (به طور مثال شبکه همکار) منشأ بگیرد. تمام سرچشمه‌های پشتیبانی شده برای به روز رسانی‌ها باید در خلاصه مشخصه محصول نشان داده شوند و مورد ارزیابی قرار گیرند.

- **آزمون** ۱: ارزیاب قبل از نصب به روز رسانی اطمینان حاصل می‌کند که به روزرسانی دارای یک امضای دیجیتال متعلق به فروشنده است. ارزیاب به روز رسانی بارگیری شده را به روشی تغییر می‌دهد که امضای دیجیتال دیگر معتبر نباشد. سپس ارزیاب تلاش می‌کند تا به روز رسانی تغییر یافته را نصب کند. ارزیاب اطمینان حاصل می‌کند که سیستم‌عامل به روز رسانی تغییر یافته را نصب نمی‌کند.
- **آزمون ۲:** ارزیاب اطمینان حاصل می‌کند که به روزرسانی دارای یک امضای دیجیتال متعلق به فروشنده است. سپس ارزیاب تلاش می‌کند تا به روز رسانی را نصب کند (یا اجاره نصب را برای ادامه می‌دهد). ارزیاب اطمینان حاصل می‌کند که سیستم‌عامل به صورت موفقیت آمیزی به روز رسانی را نصب کرده است.

۸-۲۴ اقدامات تضمین الزام کارکرد امنیتی یکپارچگی نصب و به‌روز رسانی نرم‌افزار برنامه‌کاربردی ۱ (FPT_TUD_EXT.2.1)

ارزیاب با استفاده از روش‌های اجرایی توضیح داده شده در مستندات به روز رسانی‌های نرم‌افزار برنامه‌های کاربردی را بررسی می‌کند و تعیین می‌کند که سیستم‌عامل فهرستی از به روز رسانی‌های در دسترس را ارائه می‌دهد. آزمودن این قابلیت ممکن است مستلزم قرار دادن موقت سامانه در پیکربندی‌ای متضاد با راهنمای پیکربندی امن باشد که به روز رسانی‌های خودکار را مشخص می‌کند. (ارزیاب همچنین اطمینان حاصل خواهد کرد که این پرس و جو در یک کانال قابل اعتماد به نحوی که در FTP_ITC_EXT.1 توضیح داده شده است اتفاق می‌افتد.)

۸-۲۵ اقدامات تضمین الزام کارکرد امنیتی یکپارچگی نصب و به‌روز رسانی نرم‌افزار برنامه‌کاربردی ۲ (FPT_TUD_EXT.2.2)

ارزیاب به روز رسانی را برای یک برنامه‌کاربردی آغاز خواهد کرد. بسته به برنامه‌کاربردی ممکن است متفاوت باشد، اما این کار می‌تواند از طریق وب سایت فروشنده برنامه‌کاربردی، یک فروشگاه برنامه‌های کاربردی تجاری، یا سامانه دیگری باشد. تمام سرچشمه‌های پشتیبانی شده توسط سیستم‌عامل باید در خلاصه مشخصه محصول نشان داده شوند و مورد ارزیابی قرار گیرند. با این حال، این تنها شامل ساز و کارهایی می‌شود که سیستم‌عامل قابلیت کارکردی نصب و به روز رسانی قابل اعتماد را برایش فراهم آورده است. و شامل بارگیری‌ها و نصب‌های فایل‌های دلخواه کاربر یا مدیر سیستم نمی‌باشد.

- **آزمون** ۱: ارزیاب اطمینان حاصل می‌کند که به روزرسانی یک امضای دیجیتالی دارد که به فروشنده سیستم‌عامل یا دیگر ریشه‌های قابل اعتماد از طریق سیستم‌عامل زنجیر شده است. ارزیاب به روز رسانی بارگیری شده را به روشی تغییر می‌دهد که امضای دیجیتال دیگر معتبر نباشد. سپس ارزیاب تلاش می‌کند تا به روز رسانی تغییر یافته را نصب کند. ارزیاب اطمینان حاصل می‌کند که سیستم‌عامل به روز رسانی تغییر یافته را نصب نمی‌کند.
- **آزمون ۲:** ارزیاب اطمینان حاصل می‌کند که به روزرسانی یک امضای دیجیتال دارد که متعلق به فروشنده سیستم‌عامل یا دیگر ریشه‌های قابل اعتماد از طریق سیستم‌عامل است. سپس ارزیاب تلاش می‌کند تا به روز رسانی را نصب کند (یا اجاره نصب را برای ادامه می‌دهد). ارزیاب اطمینان حاصل می‌کند که سیستم‌عامل به صورت موفقیت آمیزی به روز رسانی را نصب کرده است.

۸-۲۶ اقدامات تضمین الزام کارکرد امنیتی تولید داده ممیزی ۱ (FAU_GEN.1.1)

ارزیاب راهنمایی‌های اجرایی را بررسی کرده و اطمینان حاصل می‌کند که این راهنماها همه رویدادهای قابل ممیزی را فهرست می‌کند. ارزیاب باید بررسی کند تا مطمئن شود که هر نوع رویداد ممیزی انتخاب شده در هدف امنیتی گنجانده شده است.

ارزیاب باید توانایی سیستم‌عامل را برای تولید درست رکوردهای ممیزی با داشتن محصول تولید کننده رکوردهای ممیزی را برای رویدادهای فهرست شده در هدف امنیتی مورد آزمایش قرار دهد. این آزمون بهتر است شامل انواع نمونه‌های یک رویداد مشخص شده باشد. هنگام تأیید نتایج آزمون، ارزیاب باید اطمینان حاصل کند که رکوردهای ممیزی تولید شده در طول آزمایش با قالب مشخص شده در راهنمای اجرایی مطابقت دارد، و رشته‌های هر رکورد ممیزی ورودی مناسبی دارد.

۸-۲۷ اقدامات تضمین الزام کارکرد امنیتی تولید داده ممیزی ۲ (FAU_GEN.1.2)

ارزیاب راهنمایی‌های اجرایی را بررسی کرده و اطمینان حاصل می‌کند که این راهنماها قالبی برای رکوردهای ممیزی ارائه می‌دهد. هر قالب رکورد ممیزی‌ای باید به تنهایی با توصیف مختصری از هر رشته پوشش داده شود. ارزیاب باید اطمینان حاصل کند که رشته‌ها شامل اطلاعات مورد نیاز است.

ارزیاب باید توانایی سیستم‌عامل را برای تولید درست رکوردهای ممیزی با داشتن محصول تولید کننده رکوردهای ممیزی را برای رویدادهای فهرست شده در هدف امنیتی مورد آزمایش قرار دهد. ارزیاب باید اطمینان حاصل کند که رکوردهای ممیزی تولید شده در طول آزمایش با قالب مشخص شده در راهنمای اجرایی مطابقت دارد، و رشته‌های هر رکورد ممیزی اطلاعات مورد نیاز را فراهم می‌آورد.

۸-۲۸ اقدامات تضمین ساماندهی شکست در احراز هویت ۱ (FIA_AFL.1.1)

ارزیاب یک آستانه قابل پیکربندی مدیر سیستمی برای تلاش‌های خرابی قرار داده، یا اختصاص‌های تعیین شده هدف امنیتی را مورد توجه قرار می‌دهد. سپس ارزیاب (به ازای هر انتخاب) تلاش برای احراز هویت را با یک کلمه‌عبور، پین، یا گواهی اشتباه تا رسیدن تعداد تلاش‌ها به آستانه تکرار می‌کند. توجه داشته باشید که تلاش‌های احراز هویت و ممنوعیت باید به نحوی ثبت گردد که در FAU_GEN.1 مشخص شده است.

۸-۲۹ اقدامات تضمین الزام کارکرد امنیتی ساماندهی شکست در احراز هویت ۲ (FIA_AFL.1.2)

- **آزمون** ۱: ارزیاب مکرراً تلاش خواهد کرد تا با یک رمز عبور بد معلوم در سامانه احراز هویت کند. زمانی که به تعداد تعریف شده تلاش‌های احراز هویت شکست خورده رسید ارزیاب اطمینان حاصل می‌کند که حساب کاربری‌ای که برای آزمایش مورد استفاده قرار گرفته است اقداماتی را برای اجرا دارد که در فهرست اختصاص بالا به تفصیل توضیح داده شده است. ارزیاب اطمینان حاصل می‌کند رویدادی که در ثبت وقایع رویداد امنیتی ثبت شده است با جزئیاتی ثبت شده است که حساب کاربری این اقدامات را اعمال کرده است.
- **آزمون ۲:** ارزیاب مکرراً تلاش خواهد کرد تا با یک گواهی بد معلوم در سامانه احراز هویت کند. زمانی که به تعداد تعریف شده تلاش‌های احراز هویت شکست خورده رسید ارزیاب اطمینان حاصل می‌کند که حساب کاربری‌ای که برای آزمایش مورد استفاده قرار گرفته است اقداماتی را برای اجرا دارد که در فهرست اختصاص بالا به تفصیل توضیح داده شده است. ارزیاب اطمینان حاصل می‌کند رویدادی که در ثبت وقایع رویداد امنیتی ثبت شده است با جزئیاتی ثبت شده است که حساب کاربری این اقدامات را اعمال کرده است.
- **آزمون ۳:** ارزیاب مکرراً تلاش خواهد کرد تا هم با یک کلمه‌عبور بد و هم یک گواهی بد در سامانه احراز هویت کند. زمانی که به تعداد تعریف شده تلاش‌های احراز هویت شکست خورده رسید ارزیاب اطمینان حاصل می‌کند که حساب کاربری‌ای که برای آزمایش مورد استفاده قرار گرفته است

اقداماتی را برای اجرا دارد که در فهرست اختصاص بالا به تفصیل توضیح داده شده است. ارزیاب اطمینان حاصل می‌کند رویدادی که در ثبت وقایع رویداد امنیتی ثبت شده است با جزئیاتی ثبت شده است که حساب کاربری این اقدامات را اعمال کرده است..

۸-۳۰ اقدامات تضمین الزام کارکرد امنیتی ساز و کارهای احراز هویت چندگانه ۱ (FIA_UAU.5.1)

اگر احراز هویت نام کاربری و کلمه‌عبور انتخاب شد، ارزیاب سیستم‌عامل را با یک نام کاربری و کلمه‌عبور معلوم پیکربندی خواهد نمود و آزمون‌های زیر را انجام خواهد داد:

- **آزمون** ۱: ارزیاب تلاش می‌کند تا با استفاده از نام کاربری و کلمه‌عبور معلوم در سیستم‌عامل احراز هویت کند. ارزیاب اطمینان حاصل می‌کند که تلاش احراز هویت موفقیت آمیز است.
- **آزمون ۲:** ارزیاب تلاش می‌کند تا با استفاده از نام کاربری معلوم و کلمه‌عبور نادرست برای سیستم‌عامل احراز هویت کند. ارزیاب اطمینان حاصل می‌کند که تلاش احراز هویت ناموفق است.

اگر نام کاربری و پینی که کلید نامتقارن انتشار می‌دهد انتخاب شده باشد، ارزیاب خلاصه مشخصه محصول را برای راهنمایی در مورد انبارش محافظت شده پشتیبانی شده بررسی خواهد کرد و سپس محصول یا OE را برای برقراری پینی که انتشار کلید نامتقارن از انبارش محافظت شده (به طور مثال TPM، نشانه سخت‌افزاری، یا محیط اجرایی ایزوله شده) را فعال می‌کند که سیستم‌عامل قادر به برقراری ارتباط باشد. سپس ارزیاب آزمون‌های زیر را انجام خواهد داد:

- **آزمون** ۱: ارزیاب تلاش می‌کند تا با استفاده از نام کاربری و پین معلوم در سیستم‌عامل احراز هویت کند. ارزیاب اطمینان حاصل می‌کند که تلاش احراز هویت موفقیت‌آمیز است.

- **آزمون ۲**: ارزیاب تلاش می‌کند تا با استفاده از نام کاربری معلوم و پین نادرست برای سیستم‌عامل احراز هویت کند. ارزیاب اطمینان حاصل می‌کند که تلاش احراز هویت ناموفق است.

اگر احراز هویت گواهی X.509 انتخاب شده باشد، ارزیاب گواهی X.509v3 را برای کاربر با مجموعه رشته کاربری کلید توسعه یافته احراز هویت سرویس‌گیرنده تولید می‌کند. ارزیاب سیستم‌عامل را برای احراز هویت با گواهی X.509v3 آماده می‌کند. ارزیاب اطمینان حاصل خواهد کرد که گواهی‌ها با سیستم‌عامل از طریق FIA_X509_EXT.1.1 اعتباردهی شده‌اند سپس آزمون‌های زیر را انجام خواهد داد:

- **آزمون ۱**: ارزیاب تلاش می‌کند تا با استفاده از گواهی X.509v3 در سیستم‌عامل احراز هویت کند. ارزیاب اطمینان حاصل می‌کند که تلاش احراز هویت موفقیت‌آمیز است.
- **آزمون ۲**: ارزیاب گواهی دومی یکسانی با گواهی اول تولید می‌کند به جز کلید عمومی و هر مقداری که از کلید عمومی استخراج شده است. ارزیاب تلاش می‌کند تا با استفاده از این گواهی برای سیستم‌عامل احراز هویت کند. ارزیاب اطمینان حاصل می‌کند که تلاش احراز هویت ناموفق است.

۸-۳۱ اقدامات تضمین الزام کارکرد امنیتی اعتبارسنجی گواهی X.509 ۱ (FIA_X509_EXT.1.1)

ارزیاب اطمینان حاصل می‌کند که خلاصه مشخصه محصول توضیح می‌دهد که کجا بررسی اعتبار گواهی‌ها اتفاق می‌افتد. ارزیاب همچنین اطمینان می‌یابد که خلاصه مشخصه محصول توصیفی از الگوریتم اعتبارسنجی مسیر گواهی ارائه می‌دهد.

آزمون‌های توضیح داده شده در زیر باید پیوسته با دیگر اقدامات تضمین خدمات گواهی‌ها از جمله توابع موجود در FIA_X509_EXT.2.1 انجام شود. آزمون‌ها برای قوانین کاربری کلید توسعه یافته همراه با استفاده‌هایی که مستلزم آن قوانین است انجام شده‌اند. ارزیاب زنجیره‌ای از حداقل چهار گواهی خواهد ساخت: گواهی گره‌ای که باید مورد آزمایش قرار گیرد، دو CA میانجی، CA ریشه خود امضا شده.

- **آزمون** ۱: ارزیاب نشان خواهد داد که اعتبارسنجی یک گواهی بدون یک مسیر گواهی معتبر منجر به شکست تابع می‌شود. سپس ارزیاب گواهی یا گواهی‌ها را به گونه‌ای بارگیری خواهد کرد که CA های قابل اعتماد برای اعتبارسنجی گواهی‌ای که در تابع استفاده خواهد شد مورد نیاز هستند، و نشان می‌دهد که تابع با موفقیت اجرا شده است. سپس ارزیاب باید یکی از گواهی‌ها را حذف کند و نشان دهد که تابع با شکست روبرو بوده است.
- **آزمون ۲:** ارزیاب نشان خواهد داد که اعتبارسنجی یک گواهی منقضی شده منجر به شکست تابع می‌شود.
- **آزمون ۳**: ارزیاب آزمایش خواهد کرد که سیستم‌عامل بتواند به درستی با گواهی‌های باطل شده رفتار کند – مشروط به اینکه CRL، OCSP، یا اتصال OCSP انتخاب شده باشد، اگر چندین روش انتخاب شده باشد، آزمون باید برای هر روش انجام شود. ارزیاب ابطال گواهی گره و ابطال گواهی CA میانجی را (یعنی گواهی CA میانجی باید توسط CA ریشه باطل شده باشد) آزمایش خواهد کرد. ارزیاب اطمینان حاصل می‌کند که از یک گواهی معتبر استفاده شده است، و تابع اعتبارسنجی با موفقیت روبرو بوده است. سپس ارزیاب تلاش می‌کند تا با گواهی‌ای که باطل شده است آزمون را انجام دهد (برای هر روش انتخاب شده در انتخاب) تا اطمینان یابد وقتی گواهی دیگر معتبر نیست تابع اعتبارسنجی با شکست روبرو می‌شود.
- **آزمون ۴**: چنانچه هر گزینه OCSP انتخاب شود، ارزیاب سرور OCSP را پیکربندی خواهد کرد یا از ابزاری که انسان میانجی باشد استفاده خواهد کرد تا گواهی ارائه دهد که هدف امضای OCSP را ندارد و بررسی می‌کند که اعتبارسنجی پاسخ OCSP با شکست روبرو شود. اگر CRL انتخاب

شده باشد، ارزیاب CA را برای امضای یک CRL با گواهی‌ای که بیت کاربری کلید امضای CRL ست نشده است، پیکربندی خواهد کرد و بررسی می‌کند که اعتبارسنجی CRL با شکست روبرو شود.

- **آزمون ۵**: ارزیاب هر بایتی را در هشت بایت اول گواهی تغییر خواهد داد و نشان می‌دهد که اعتبارسنجی گواهی با شکست روبرو می‌شود. (گواهی باید به درستی در تجزیه شدن شکست بخورد.)
- **آزمون ۶**: ارزیاب هر بایتی را در آخرین بایت گواهی تغییر خواهد داد و نشان می‌دهد که اعتبارسنجی گواهی با شکست روبرو می‌شود. (امضا روی گواهی نباید معتبر باشد.)
- **آزمون ۷**: ارزیاب هر بایتی را در کلید عمومی گواهی تغییر خواهد داد و نشان می‌دهد که اعتبارسنجی گواهی با شکست روبرو می‌شود. (امضا روی گواهی نباید معتبر باشد.)

۳۲-۸ اقدامات تضمین الزام کارکرد امنیتی اعتبارسنجی گواهی X.509 ۲ (FIA_X509_EXT.1.2)

آزمون‌های توضیح داده شده باید همراه با دیگر اقدامات تضمین خدمات گواهی‌ها از جمله توابع موجود در FIA_X509_EXT.2.1 انجام شود. ارزیاب زنجیره‌ای از حداقل چهار گواهی خواهد ساخت: گواهی گره‌ای که باید مورد آزمایش قرار گیرد، دو CA میانجی، CA ریشه خود امضا شده.

- **آزمون ۱**: ارزیاب یک مسیر گواهی خواهد ساخت به طوریکه گواهی CA صادر کننده گواهی سیستم‌عامل شامل بسط محدودیت‌های اصلی نباشد. اعتبارسنجی مسیر گواهی شکست می‌خورد.

- **آزمون ۲:** ارزیاب یک مسیر گواهی خواهد ساخت به طوریکه گواهی CA صادر کننده گواهی سیستم‌عامل شامل پرچم CA باشد که در بسط محدودیت‌های اصلی تنظیم نشده است. اعتبارسنجی مسیر گواهی شکست می‌خورد.
- **آزمون ۳**: ارزیاب یک مسیر گواهی خواهد ساخت به طوریکه گواهی CA صادر کننده گواهی سیستم‌عامل شامل پرچم CA باشد که در بسط محدودیت‌های اصلی "درست" تنظیم شده است. اعتبارسنجی مسیر گواهی موفقیت‌آمیز خواهد بود

۸-۳۳ اقدامات تضمین الزام کارکرد امنیتی احرازهویت گواهی X.509 ۱ (FIA_X509_EXT.2.1)

ارزیاب برنامه‌کاربردی‌ای را به دست می‌آورد یا توسعه می‌دهد که از ساز و کار OS TLS با یک گواهی X.509v3 استفاده کند. ارزیاب سپس برنامه‌کاربردی را اجرا کرده و اطمینان می‌یابد که گواهی ارائه شده برای احراز هویت اتصال به کار رفته است.

ارزیاب فعالیت را برای هر انتخاب فهرست شده دیگر تکرار خواهد کرد.

۸-۳۴ اقدامات تضمین الزام کارکرد امنیتی ارتباط کانال قابل اعتماد ۱ (FTP_ITC_EXT.1.1)

ارزیاب سیستم‌عامل را برای ارتباط با دیگر محصولات قابل اعتماد IT به نحوی که در انتخاب دوم شناسایی شده است پیکربندی خواهد کرد. ارزیاب هنگامی که سیستم‌عامل با هر یک از سرورهای مشخص شده در انتخاب دوم ارتباط برقرار می‌کند، بر ترافیک شبکه نظارت خواهد کرد. ارزیاب اطمینان حاصل خواهد کرد که برای هر نشستی یک کانال قابل اعتماد مطابق با پروتکل‌های شناسایی شده است در انتخاب اول تعیین شده است.

۸-۳۵ اقدامات تضمین الزام کارکرد امنیتی مسیر قابل‌اعتماد ۳ (FTP_TRP.1.3)

ارزیاب خلاصه مشخصه محصول را برای تعیین این موضوع مورد بررسی قرار می‌دهد که آیا روش‌های مدیر سیستمی از راه دور سیستم‌عامل همراه با نحوه محافظت از این ارتباطات نشان داده شده‌اند. ارزیاب همچنین تصدیق می‌کند که همه پروتکل‌های فهرست شده در خلاصه مشخصه محصول در پشتیبانی از مدیر سیستمی سیستم‌عامل با پروتکل‌های مشخص شده در الزام سازگارند و در الزامات هدف امنیتی گنجانده شده‌اند. ارزیاب همچنین تأیید خواهد کرد که راهنمای عملیاتی شامل دستورالعمل‌هایی برای برقراری نشست‌های اجرایی برای هر روش پشتیبانی شده است. ارزیاب همچنین آزمون‌های زیر را انجام خواهد داد:

- **آزمون ۱**: ارزیاب اطمینان حاصل خواهد کرد که ارتباطات با استفاده از هر روش مدیر سیستمی از راه دور در طول دوره ارزیابی مورد آزمون قرار گرفته است، ارتباطات به نحوی که در راهنمای عملیاتی توضیح داده شده است تنظیم شده است و اطمینان می‌یابد که ارتباطات موفقیت آمیز است.
- **آزمون ۲**: برای هر روش مدیر سیستمی از راه دور پشتیبانی شده، ارزیاب راهنمای عملیاتی را دنبال می‌کند تا اطمینان یابد که هیچ واسط در دسترسی نیست که بتواند توسط کاربر از راه دور برای برقراری نشست‌های اجرایی از راه دور مورد استفاده قرار گیرد بدون اینکه مسیر قابل اعتماد فراخوانی شود.
- **آزمون ۳**: ارزیاب اطمینان حاصل خواهد کرد که برای هر روش مدیر سیستمی از راه دور، داده کانال در متن خام ارسال نشده است.
- **آزمون ۴**: ارزیاب اطمینان حاصل خواهد کرد که برای هر روش مدیر سیستمی از راه دور، تغییر داده کانال توسط سیستم‌عامل شناسایی شده است.

پیوست ۱ الزامات اختیاری

همانگونه که در بخش ۲ نشان داده شد، الزامات ابتدایی (آن‌هایی که باید توسط سیستم‌عامل اعمال شوند) در متن این پروفایل حفاظتی گنجانده شد. علاوه بر این، سه نوع الزامات دیگر در پیوست آ، پیوست ب و پیوست ج مشخص شده‌اند. اولین نوع (در این پیوست) الزاماتی هستند که می‌توانند در هدف امنیتی گنجانده شوند اما برای اینکه یک سیستم‌عامل ادعای انطباق با این پروفایل حفاظتی را داشته باشد مورد نیاز نیست. نوع دوم (در پیوست ب) الزاماتی مبتنی بر انتخاب‌هایی در متن پروفایل حفاظتی هستند: چنانچه انتخاب معینی انجام شود، الزامات افزوده در پیوست باید به حساب آورده شود. سومین نوع (در پیوست ج) مؤلفه‌هایی هستند که برای انطباق با این پروفایل حفاظتی مورد نیاز نیستند، اما باید در الزامات اصلی در نسخه‌های آینده این پروفایل حفاظتی گنجانده شوند، بنابراین اتخاذ آن‌ها توسط فروشندگان مورد تشویق است. توجه داشته باشید که نویسنده هدف امنیتی مسئول اطمینان یافتن از این موضوع است که الزاماتی که ممکن است با الزاماتی مرتبط باشد که در پیوست آ، پیوست ب و پیوست ج فهرست نشده‌اند (به طور مثال؛ الزامات FMT-type) در هدف امنیتی گنجانده شده‌اند.

جدول ۴ الزامات اختیاری

شماره	نام الزام	الزام
۳۸	**پروتکل سرویس‌گیرنده TLS ۱**	FCS_TLSC_EXT.4.1
۳۹	**بنرهای دسترسی محصول پیش‌فرض ۱**	FTA_TAB.1.1

۱- کلاس پشتیبانی رمزنگاری

شماره الزام	نام الزام
۳۸	**پروتکل سرویس‌گیرنده TLS ۱**
سیستم‌عامل باید احراز هویت دو طرفه را با استفاده از گواهی‌های X.509v3 پشتیبانی کند.	

نکته کاربردی ۲۷: اســتفاده از گواهی‌های X.509v3 برای TLS در FIA_X509_EXT.2.1 مورد توجه قرار گرفته اســت. این الزام می‌افزاید که یک ســرویس‌گیرنده باید قادر به ارائه یک گواهی برای سرور TLS به منظور احراز هویت دو طرفه TLS باشد.

اقدامات تضمین

ارزیاب اطمینان می‌یابد که توضـیحات خلاصـه مشخصه محصول موردنیاز برای هر FIA_X509_EXT.2.1 شامل استفاده از گواهی‌های سمت سرویس‌گیرنده برای احراز هویت دو طرفه TLS می‌باشد.

ارزیاب تأیید خواهد کرد که راهنمایی‌های ســند راهنمای اجرایی مورد نیاز برای هر FIA_X509_EXT.2.1 شــامل دســتورالعمل‌هایی برای پیکربندی گواهی‌های سمت سرویس‌گیرنده برای احراز هویت دو طرفه TLS می‌باشد.

ارزیاب همچنین آزمون زیر را انجام خواهد داد:

ســرور را برای احراز هویت دو طرفه مورد نیاز پیکربندی کرده و سپس یک بایت را در یک رشتهCA در پیام دست‌داد درخواست گواهی سرور تغییر می‌دهد. رشته CA تغییر کرده نباید CA استفاده شده برای امضای گواهی سرویس‌گیرنده باشد. ارزیاب بررسی خواهد کرد که اتصال ناموفق بوده است.

۲- کلاس دسترسی به هدف ارزیابی

شماره الزام	نام الزام
۳۹	**بنرهای دسترسی محصول پیش‌فرض ۱**
قبل از برقراری یک نشست کاربری، سیستم‌عامل باید یک پیام هشدار دهنده توصیه‌ای با توجه به استفاده غیر مجاز از سیستم‌عامل را نمایش دهد.	

اقدامات تضمین

ارزیاب سیستم‌عامل را برای هر دستورالعملی در راهنمای سیستم‌عامل پیکربندی خواهد کرد تا پیام هشدار دهنده توصیه‌ای "TEST TEST" پیام هشدار TEST" را نمایش دهد. ارزیاب سپس از سامانه خارج شده و تأیید خواهد کرد که پیام توصیه‌ای قبل از اینکه ورود به سامانه بتواند اتفاق بیفتد نمایش داده شده است.

پیوست ۲ الزامات مبتنی بر انتخاب

همانگونه که در مقدمه این پروفایل حفاظتی نشان داده شده است، الزامات اساسی (آن‌هایی که باید توسط سیستم‌عامل یا سکوی آن ایفا شوند) در متن این پروفایل حفاظتی گنجانده شده است. در اینجا الزامات افزوده ای بر اساس انتخاب‌هایی که در متن پروفایل حفاظتی انجام می‌شوند آورده شده‌است: چنانچه انتخاب‌های معینی انجام شود، نیاز است تا الزامات افزوده زیر گنجانده شود.

جدول ۵ الزامات مبتنی بر انتخاب

شماره	نام الزام	الزام
۴۰	**پیاده‌سازی DTLS ۱**	FCS_DTLS_EXT.1.1
۴۱	**پیاده‌سازی DTLS ۲**	FCS_DTLS_EXT.1.2
۴۲	**پروتکل سرویس‌گیرنده TLS ۱**	FCS_TLSC_EXT.2.1

۱- کلاس پشتیبانی رمزنگاری

شماره الزام	نام الزام
۴۰	**پیاده‌سازی DTLS ۱**
سیستم‌عامل باید پروتکل DTLS را مطابق با [**انتخاب**: *DTLS 1.0 (RFC 4347)*، *DTLS 1.2 (RFC 6347)*] پیاده‌سازی کند. ***این الزام به انتخاب FTP_ITC_EXT.1.1 بستگی دارد.*** اقدامات تضمین:	

- **آزمون** ۱: ارزیاب تلاش می‌کند تا اتصالی با سرور DTLS برقرار کند، ترافیک را با آنالیزور بسته مشاهده کند، و تأیید کند که اتصال موفق بوده است و این ترافیک به عنوان DTLS شناسایی شده است.

آزمون‌های دیگر همراه با اقدامات تضمین فهرست شده برای FCS_TLSC_EXT.1 انجام شده‌اند.

۴۱	**پیاده‌سازی DTLS ۲**

سیستم‌عامل باید الزامات در TLS (FCS_TLSC_EXT.1) را برای پیاده‌سازی DTLS اجرا کند، به جز مواردی که تغییرات با توجه به DTLS 1.2 (RFC 6347) مجاز است.

این الزام به انتخاب FTP_ITC_EXT.1.1 بستگی دارد.

نکته کاربردی ۲۸: تفاوت‌های میان DTLS 1.2 و TLS 1.2 در RFC 6347 تعیین شده است. وگرنه پروتکل‌ها یکسان هستند. به طور خاص، برای مشخصات امنیتی کاربرد پذیر تعریف شده در توابع هدف امنیتی، این دو پروتکل متفاوت نیستند. بنابراین، همه نکات کاربردی و اقدامات تضمین که برای TLS فهرست شده‌اند برای پیاده‌سازی DTLS به کار می‌رود.

۴۲	**پروتکل سرویس‌گیرنده TLS ۱**

سیستم‌عامل باید بسط خم‌های بیضوی پشتیبانی شده در سلام سرویس‌گیرنده را با خم‌های NIST زیر ارائه دهد: [**انتخاب**: *secp256r1*، *secp384r1*، *secp521r1*] و هیچ خم دیگری.

این الزام به انتخاب FTP_ITC_EXT.1.1 بستگی دارد.

نکته کاربردی ۲۹: این الزام خم‌های بیضوی مجاز برای احراز هویت و توافق کلید را محدود به خم‌های NIST از FCS_COP.1(3) و FCS_CKM.1 و FCS_CKM.2 می‌کند. این بسط برای سرویس‌گیرنده‌های پشتیبانی کننده از رشته رمزهای منحنی بیضوی مورد نیاز است.

اقدامات تضمین:

ارزیاب بررسی خواهد کرد که خلاصه مشخصه محصول بسط خم‌های بیضوی پشتیبانی شده و اینکه رفتار مورد نیاز به صورت پیش فرض انجام می‌شود یا ممکن است پیکربندی شده باشد را توضیح دهد. چنانچه خلاصه مشخصه محصول نشان دهد که بسط خم‌های بیضوی پشتیبانی شده باید برای برآوردن الزام پیکربندی شود، ارزیاب بررسی خواهد کرد تا راهنمایی سند راهنمای اجرایی پیکربندی بسط خم‌های بیضوی پشتیبانی شده را شامل شده باشد.

ارزیاب آزمون زیر را انجام خواهد داد:

ارزیاب سرور را برای اجرای یک پیام تبادل کلید ECDHE در اتصال TLS با استفاده از خم ECDHE پشتیبانی نشده (برای مثال، P-192) پیکربندی خواهد کرد و باید بررسی کند که سیستم‌عامل بعد از دریافت پیام دست‌داد تبادل کلید سرور، اتصال را قطع می‌کند.

پیوست ۳ الزامات هدف

این پیوست شامل الزاماتی است که قابلیت کارکرد امنیتی را مشخص می‌کند که تهدیدات را نیز مورد توجه قرار می‌دهد. نظر به اینکه این الزامات قابلیت‌های امنیتی‌ای را توضیح می‌دهند که هنوز به صورت گسترده در فناوری تجاری در دسترس نیستند در حال حاضر در متن این پروفایل حفاظتی اجباری نشده‌اند. هر چند، این الزامات ممکن است در هدف امنیتی گنجانده شوند به طوری که سیستم‌عامل هنوز با این پروفایل حفاظتی انطباق داشته باشد، و انتظار می‌رود که در اسرع وقت گنجانده شوند.

جدول ۶ الزامات هدف

شماره	نام الزام	الزام
۴۳	**پروتکل سرویس‌گیرنده TLS ۱**	FCS_TLSC_EXT.3
۴۴	**خط‌مشی‌های محدود کردن نرم‌افزار ۱**	FPT_SRP_EXT.1
۴۵	**نوشتن یا (XOR) اجرای صفحات حافظه ۱**	FPT_W^X_EXT.1

۱- کلاس پشتیبانی رمزنگاری

شماره الزام	نام الزام
۴۳	**پروتکل سرویس‌گیرنده TLS ۱**
سیستم‌عامل باید بسط الگوریتم– امضا را در سلام سرویس‌گیرنده با مقدار الگوریتم‌های – امضای – پشتیبانی شده موجود در الگوریتم‌های چکیده‌ساز زیر ارائه دهد: [**انتخاب**: *SHA256*، *SHA384*، *SHA512*] و هیچ الگوریتم چکیده‌ساز دیگری.	

نکته کاربردی ۳۰: این الزام الگوریتم‌های چکیده‌ساز پشتیبانی شده برای هدف درستی‌سنجی امضای دیجیتالی توسط سرویس‌گیرنده را محدود می‌کند و سرور را به چکیده‌سازهای پشتیبانی شده برای هدف تولید امضای دیجیتال توسط سرور محدود می‌کند. بسط الگوریتم – امضا تنها توسط TLS 1.2 پشتیبانی شده است.

اقدامات تضمین:

ارزیاب بررسی خواهد کرد که خلاصه مشخصه محصول بسط الگوریتم – امضا و اینکه رفتار مورد نیاز به صورت پیش فرض انجام می‌شود یا پیکربندی شده است را توضیح دهد. چنانچه خلاصه مشخصه محصول نشان دهد که بسط الگوریتم – امضا باید برای برآوردن الزام پیکربندی شود، ارزیاب بررسی خواهد کرد تا راهنمایی سند راهنمای اجرایی پیکربندی بسط الگوریتم – امضا را در بر گرفته باشد.

ارزیاب آزمون زیر را نیز انجام خواهد داد:

ارزیاب سرور را برای ارسال یک گواهی در اتصال TLS پیکربندی خواهد کرد که با توجه به شمارش الگوریتم چکیده‌ساز سرویس‌گیرنده در بسط الگوریتم – امضا پشتیبانی نشده است (برای مثال، ارسال یک گواهی با امضای SHA-1). ارزیاب تأیید خواهد کرد که سیستم‌عامل بعد از دریافت پیام دست داد گواهی سرور اتصال را قطع می‌کند.

۲- کلاس حفاظت از توابع هدف امنیتی

شماره الزام	نام الزام
۴۴	**خط‌مشی‌های محدود کردن نرم‌افزار ۱**
سیستم‌عامل باید اجرا را تنها محدود به برنامه‌هایی کند که با انتخاب مشخص شده توسط مدیر سیستم انطباق دارد [**انتخاب**: *مسیر فایل،* *امضای دیجیتال فایل،* *نسخه،*	

چکیده‌ساز،

*[**اختصاص**: دیگر مشخصه‌ها]*

[

نکته کاربردی ۳۱: اختصـــاص پیاده‌ســـازی‌هایی را تأیید می‌کند که یک ســـطح حداقلی از دانه دانه بودن را مانند یک مجلد فراهم آورد. محدودیت تنها در برابر اجرای مســـتقیم برنامه‌های اجرایی اســـت. این محدودیت مفســـرهایی را که ممکن اســـت داده را به عنوان ورودی بگیرند منع نمی‌کند، حتی اگر این داده بتواند متعاقباً منجر به محاسبات دلخواه شود.**اقدامات تضمین:**

ارزیاب بررسی خواهد کرد که خلاصه مشخصه محصول بسط الگوریتم – امضا و اینکه رفتار مورد نیاز به صورت پیش فرض انجام می‌شود یا پیکربندی شده است را توضیح دهد. چنانچه خلاصه مشخصه محصول نشان دهد که بسط الگوریتم – امضا باید برای برآوردن الزام پیکربندی شود، ارزیاب بررسی خواهد کرد تا راهنمایی سند راهنمای اجرایی پیکربندی بسط الگوریتم – امضا را در بر گرفته باشد.

ارزیاب آزمون زیر را نیز انجام خواهد داد:

ارزیاب سرور را برای ارسال یک گواهی در اتصال TLS پیکربندی خواهد کرد که با توجه به شمارش الگوریتم چکیده‌ساز سرویس‌گیرنده در بسط الگوریتم – امضا پشتیبانی نشده است (برای مثال، ارسال یک گواهی با امضای SHA-1). ارزیاب تأیید خواهد کرد که سیستم‌عامل بعد از دریافت پیام دست داد گواهی سرور اتصال را قطع می‌کند.

اقدامات تضمین

برای هر انتخاب مشخص شده در هدف امنیتی، ارزیاب اطمینان حاصل خواهد کرد که آزمون‌های مربوطه منجر به یک خروجی منفی خواهد شد (به عبارت دیگر، اقدام منجر به این می‌شود که سیستم‌عامل اجازه ارزیاب برای انجام عمل را رد کند):

- **آزمون** ۱: ارزیاب سیستم‌عامل را تنها برای اجازه اجرای کد از دایرکتوری‌های سیستم‌عامل اصلی پیکربندی خواهد کرد. ارزیاب سپس تلاش می‌کند تا کد را از دایرکتوری‌ای که در فهرست مجاز است اجرا کند. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا شده است.
- **آزمون** ۲: ارزیاب سیستم‌عامل را تنها برای اجازه اجرای کد از دایرکتوری‌های سیستم‌عامل اصلی پیکربندی خواهد کرد. ارزیاب سپس تلاش می‌کند تا کد را از دایرکتوری‌ای که در فهرست غیر مجاز است اجرا کند. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا نشده است.
- **آزمون** ۳: ارزیاب سیستم‌عامل را تنها برای اجازه اجرای کدی که توسط فروشنده سیستم‌عامل برای اجرا امضا شده است پیکربندی خواهد کرد. ارزیاب سپس تلاش می‌کند تا کد امضا شده توسط فروشنده سیستم‌عامل را اجرا کند. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا شده است.
- **آزمون** ۴: ارزیاب سیستم‌عامل را تنها برای اجازه کدی که توسط فروشنده سیستم‌عامل برای اجرا امضا شده است پیکربندی خواهد کرد. ارزیاب سپس تلاش می‌کند تا کدی را اجرا کند که توسط دیگر مجوز دیجیتالی امضا شده است. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا نشده است.
- **آزمون** ۵: ارزیاب سیستم‌عامل را برای اجازه اجرای یک برنامه‌کاربردی خاص بر اساس نسخه پیکربندی خواهد کرد. ارزیاب سپس تلاش می‌کند تا همان نسخه برنامه‌کاربردی را اجرا کند. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا شده است.
- **آزمون** ۶: ارزیاب سیستم‌عامل را برای اجازه اجرای یک برنامه‌کاربردی خاص بر اساس نسخه پیکربندی خواهد کرد. ارزیاب سپس تلاش می‌کند تا یک نسخه قدیمی‌تر برنامه‌کاربردی را اجرا کند. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا نشده است.
- **آزمون** ۷: ارزیاب سیستم‌عامل را برای اجازه اجرای مبتنی بر چکیده‌ساز یک برنامه‌کاربردی اجرایی پیکربندی خواهد کرد. ارزیاب سپس تلاش می‌کند تا برنامه‌کاربردی را با چکیده‌ساز منطبق اجرا کند. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا شده است.

آزمون ۸: ارزیاب سیستم‌عامل را برای اجازه اجرای مبتنی بر چکیده‌ساز یک برنامه‌کاربردی اجرایی پیکربندی خواهد کرد. ارزیاب سپس برنامه‌کاربردی را به روشی تغییر می‌دهد که چکیده‌ساز برنامه‌کاربردی تغییر یابد. ارزیاب سپس تلاش می‌کند تا برنامه‌کاربردی را با چکیده‌ساز منطبق اجرا کند. ارزیاب اطمینان حاصل می‌کند که کدی که اقدام به اجرای آن شده است، اجرا نشده است.

۴۵	**نوشتن یا (XOR) اجرای صفحات حافظه ۱**

سیستم‌عامل باید از اختصاص هر منطقه حافظه با هر دو مجوز نوشتن یا اجرا به جز برای [**اختصاص**: فهرستی از استثنائات] جلوگیری کند.

نکته کاربردی ۳۲: درخواست یک نگاشت حافظه با هر دو مجوز نوشتن و اجرا منجر به خرابکاری و واژگونی محافظت از سکوی ارائه شده توسط ممانعت از اجرای داده می‌شود. اگر سیستم‌عامل هیچ استثنائی ارائه ندهد (مانند همگردانی به موقع[۸۲])، باید "هیچ استثنائی" در اختصاص نشان داده شود. تشخیص کامل این الزام نیازمند پشتیبانی سخت‌افزاری است، اما به طور متداول در دسترس است.

اقدامات تضمین:

ارزیاب مستندات توسعه‌دهنده ارائه شده توسط فروشنده را مورد بازرسی قرار خواهد داد و بررسی می‌کند که هیچ نگاشت حافظه‌ای با مجوز نوشتن و اجرا قابل ایجاد نباشد مگر برای مواردی که در اختصاص فهرست شده است.

- **آزمون** ۱: ارزیاب برنامه آزمونی را به دست خواهد آورد یا می‌سازد که در تلاش برای اختصاص حافظه‌ای است که هم قابل نوشتن باشد و هم قابل اجرا. ارزیاب برنامه را اجرا خواهد کرد و تأیید می‌کند که اختصاص حافظه‌ای که هم قابل نوشتن و هم قابل اجرا باشد با شکست روبرو شده است.

[۸۲] Just-in-time compilation

- **آزمون ۲:** ارزیاب برنامه آزمونی را به دست خواهد آورد یا می‌سازد که حافظه‌ای را اختصاص می‌دهد که قابل اجراست و سپس مجوزهای نوشتن یا تغییر افزوده را روی آن حافظه درخواست می‌کند. ارزیاب برنامه را اجرا خواهد کرد و تأیید می‌کند که در هیچ زمانی در طول مدت حیات فرایند حافظه هم قابل نوشتن و هم قابل اجرا نیست.

آزمون ۳: ارزیاب برنامه آزمونی را به دست خواهد آورد یا می‌سازد که حافظه‌ای را اختصاص می‌دهد که قابل نوشتن است و سپس مجوزهای اجرای افزوده را روی آن حافظه درخواست می‌کند. ارزیاب برنامه را اجرا خواهد کرد و تأیید می‌کند که در هیچ زمانی در طول مدت حیات فرایند حافظه هم قابل نوشتن و هم قابل اجرا نیست.

پیوست ۴ الزامات برآورده شده ذاتی

این پیوست الزاماتی را فهرست می‌کند که بهتر است توسط محصولاتی که به صورت موفقیت‌آمیز بر اساس این پروفایل حفاظتی ارزیابی شده‌اند برآورده شده در نظر گرفته می‌شود. هر چند، این الزامات به‌صراحت به‌عنوان الزامات کارکرد امنیت مشخص نشده‌اند و بهتر است در هدف امنیتی گنجانده نشوند. این الزامات به عنوان الزامات کارکرد امنیتی مستقل گنجانده نشده‌اند چرا که این باعث افزایش زمان، هزینه و پیچیدگی ارزیابی می‌شود. این رویکرد توسط قسمت ۱ معیار مشترک، **۸,۲ وابستگی‌های میان مؤلفه‌ها** تصویب شده است.

این اطلاعات منافعی برای اقدامات مهندسی سامانه‌ها به دنبال دارد که برای گنجاندن کنترل‌های امنیتی خاصی فراخوانی می‌شوند. ارزیابی بر اساس پروفایل حفاظتی شواهدی ارائه می‌دهد که این کنترل‌ها وجود دارند و مورد ارزیابی قرار گرفته‌اند.

جدول ۷ الزامات برآورده شده ذاتی

الزامات امنیتی		منطق برای برآوردن
زمانبندی احراز هویت	FIA_UAU.1	این الزام به‌طور ضمنی مستلزم این است که سیستم‌عامل همه اقدامات ضروری را انجام دهد از جمله آن‌هایی که در طرف کاربری است که احراز اصالت نشده است، تا احراز اصالت شود؛ بنابراین گنجاندن این اقدامات به عنوان اختصاص و آزمون جداگانه تکراری است.
زمانبندی شناسایی	FIA_UID.1	این الزام به‌طور ضمنی مستلزم این است که سیستم‌عامل همه اقدامات ضروری را انجام دهد از جمله آن‌هایی که در طرف کاربری است که شناسایی نشده است، تا احراز اصالت شود؛ بنابراین گنجاندن این اقدامات به عنوان اختصاص و آزمون جداگانه تکراری است.

نقش‌های امنیتی	FMT_SMR.1	این الزام، توابع مدیریتی مبتنی بر نقش را مشخص می‌کند که به طور ضمنی حساب‌های کاربری و حساب‌های ممتاز را تعریف می‌کند؛ بنابراین، گنجاندن الزامات نقش جداگانه تکراری است.
مهرهای زمانی قابل اطمینان	FPT_STM.1	این الزام، به‌طور ضمنی مستلزم این است که سیستم‌عامل نشان‌های زمانی را با سوابق ممیزی مرتبط سازد؛ بنابراین گنجاندن الزامات نشان‌های زمانی جداگانه تکراری است.
قفل کردن نشست آغاز شده توابع هدف امنیتی	FTA_SSL.1	این الزام، الزاماتی را برای مدیریت قفل کردن نشست تعریف می‌کند؛ بنابراین گنجاندن الزام قفل کردن نشست جداگانه تکراری است.
قفل کردن نشست آغاز شده توسط کاربر	FTA_SSL.2	این الزام، الزاماتی را برای قفل کردن نشست آغاز شده کاربر تعریف می‌کند؛ بنابراین گنجاندن الزام قفل کردن نشست جداگانه تکراری است.
انبارش دنباله ممیزی محافظت شده	FAU_STG.1	این الزام، الزاماتی را برای محافظت از ثبت وقایع ممیزی تعریف می‌کند؛ بنابراین گنجاندن الزامات قفل کردن نشست جداگانه تکراری است.
ارتباط شناسه کاربر	FAU_GEN.2	این الزام به‌طور ضمنی مستلزم آن است که سیستم‌عامل هر حساب کاربری مرتبط با هر رویداد را ثبت کند؛ بنابراین، گنجاندن الزامات جداگانه برای ارتباط دادن حساب کاربری با هر رویداد تکراری است.
بازنگری ممیزی	FAU_SAR.1	این الزام مستلزم آن است که ثبت وقایع ممیزی (و دیگر موجودیت‌های غیرفعال) از خوانده شدن توسط کاربران غیر ممتاز محافظت شود؛ بنابراین گنجاندن یک الزام جداگانه برای حفاظت از تنها اطلاعات ممیزی تکراری است.

پیوست ۵ مستندسازی آنتروپی و ارزیابی

این پیوست اطلاعات تکمیلی مورد نیاز برای منبع آنتروپی مورد استفاده توسط سیستم‌عامل را توصیف می‌کند.

مستندسازی منبع آنتروپی بهتر است به اندازه کافی با جزئیات باشد که بعد از خواندن، ارزیاب منبع آنتروپی و اینکه چرا برای فراهم کردن آنتروپی کافی قابل اتکا است را به طور کامل درک کند. این سند باید شامل چندین بخش مفصل باشد: توصیف طراحی، استدلال آنتروپی، شرایط عملیاتی، و آزمون سلامت. این سند نیازی نیست که قسمتی از خلاصه مشخصه محصول باشد.

توصیف طراحی

مستندات باید شامل طراحی منبع آنتروپی به عنوان یک کل، از جمله تعامل همه مؤلفه‌های منبع آنتروپی باشد. هر گونه اطلاعاتی که در خصوص طراحی قابل اشتراک گذاری باشد بهتر است برای هر منبع آنتروپی طرف سوم که در محصول موجود است نیز گنجانده شود.

مستندات عملیات منبع آنتروپی را توضیح خواهد داد که نحوه تولید آنتروپی، و نحوه کسب داده‌های (خام) پردازش نشده از درون منبع آنتروپی برای اهداف آزمایش را در بر می‌گیرد. مستندات باید سر تا سر طراحی منبع آنتروپی قدم بردارد تا نشان دهد آنتروپی از کجا می‌آید، بعد از آن خروجی آنتروپی کجا می‌رود، هر گونه خروجی خام بعد از پردازش (چکیده‌ساز، XOR و غیره) آیا/کجا ذخیره می‌شود، و در نهایت، چگونه خروجی‌ای از منبع آنتروپی است. همچنین هر شرطی که در فرایند وضع می‌شود (به طور مثال، مسدود کردن) بهتر است در طراحی منبع آنتروپی توضیح داده شود. نمودارها و مثال‌ها مورد تشویق قرار می‌گیرند.

طراحی همچنین باید شامل شرحی از محتوای مرزهای امنیتی منبع آنتروپی و توصیفی باشد از چگونگی حصول اطمینان توسط مرز امنیتی از اینکه که مهاجم خارج از مرز نمی‌تواند بر نرخ آنتروپی تأثیر بگذارد.

در صورت پیاده‌سازی، توصیف طراحی باید شامل توصیفی باشد از نحوه‌ای که برنامه‌های کاربردی طرف سوم می‌توانند آنتروپی را به تولید کننده بیت تصادفی بیفزایند. توصیفی از هر حالت تولید کننده بیت تصادفی ذخیره کننده بین خاموشی و روشن باید گنجانده شود.

استدلال آنتروپی

باید استدلالی فنی در مورد اینکه غیر قابل پیش‌بینی بودن در منابع از کجا می‌آید و چرا به منبع آنتروپی اعتماد می‌شود که تحویل دهنده آنتروپی کافی برای استفاده‌هایی است که از خروجی RGB (با این سیستم‌عامل خاص) می‌شود. این استدلال شامل توصیفی از نرخ حداقل آنتروپی مورد انتظار (یعنی حداقل آنتروپی (به بیت) در هر بیت یا بایت از داده منبع) است و توضیح می‌دهد که آنتروپی کافی در حال رفتن به فرایند مقداردهی اولیه (بذرپاشی) تصادفی کننده سیستم‌عامل است. این مبحث قسمتی از استدلال برای این موضوع خواهد بود که چرا منبع آنتروپی برای تولید بیت‌ها با آنتروپی قابل اتکا است.

میزان اطلاعات ضروری برای توجیه نرخ حداقل آنتروپی مورد انتظار بستگی به نوع منبع آنتروپی موجود در محصول دارد.

انتظار می‌رود برای توسعه دهنده‌ای که منابع آنتروپی را فراهم آورده است، به منظور توجیه نرخ حداقل آنتروپی، تعداد زیادی از بیت‌های منبع خام جمع‌آوری شده، آزمون‌های آماری انجام شود، و نرخ حداقل آنتروپی از آزمون‌های آماری تعیین گردد. در حالی که هیچ آزمون آماری‌ای در حال حاضر مورد نیاز نیست، انتظار می‌رود که برخی از آزمون‌ها برای تعیین میزان آنتروپی حداقلی در هر خروجی ضروری باشد.

برای منابع آنتروپی ارائه شده توسط طرف سوم، که در آن فروشنده سیستم‌عامل دسترسی برای طراحی و منبع داده آنتروپی خام را محدود کرده است، مستندات برآوردی از میزان حداقل آنتروپی به دست آمده از این منبع طرف سوم را نشان دهد. برای فروشنده قابل قبول است که یک مقداری از آنتروپی حداقلی را "فرض" کند، با این حال، این مفروضات باید به وضوح در مستندات ارائه شده بیان شود. به خصوص، برآورد آنتروپی حداقلی باید مشخص شود و مفروضات در هدف امنیتی گنجانده شود.

بدون در نظر گرفتن نوع منبع آنتروپی، استدلال همچنین شامل این موضوع خواهد بود که چگونه تولید کننده بیت تصادفی قطعی با آنتروپی بیان شده در هدف امنیتی مقدار دهی اولیه خواهد شد، برای مثال با بررسی این موضوع که نرخ حداقل آنتروپی با مقداری از داده منبع مورد استفاده برای مقداردهی اولیه (بذرپاشی) تولید کننده بیت تصادفی قطعی ضرب شده یا اینکه نرخ آنتروپی مورد انتظار بر اساس مقدار داده منبع به صورت صریح بیان شده و با نرخ آماری مقایسه گردیده است. چنانچه میزان داده منبع مورد استفاده برای مقداردهی اولیه (بذرپاشی) تولید کننده بیت تصادفی قطعی مشخص نباشد یا نرخ محاسبه شده به صراحت به نقطه آغاز مرتبط نباشد، مستندات به طور کامل در نظر گرفته نخواهند شد.

استدلال آنتروپی نباید شامل هرگونه داده اضافه شده از هیچ برنامه‌کاربردی طرف سوم یا از هیچ حالت ذخیره کننده بین راه‌اندازی‌های مجدد باشد.

شرایط عملیات

نرخ آنتروپی ممکن است تحت تأثیر شرایط خارج از خود منبع آنتروپی باشد. برای مثال، ولتاژ، فرکانس، دما، و زمان سپری شده پس از روشنی تنها تعداد کمی از عواملی هستند که ممکن است عملیات منبع آنتروپی را تحت تأثیر قرار دهند. به این ترتیب، مستندات شامل طیفی از شرایط عملیاتی است که تحت آن انتظار می‌رود منبع آنتروپی داده تصادفی تولید کند. این مستندات به صورت واضح اقدامات اتخاذ شده در طراحی سامانه را توضیح خواهد داد تا اطمینان حاصل شود که منبع آنتروپی به عملکرد خود تحت آن شرایط ادامه می‌دهد. به طور مشابه، مستندات باید شرایطی را توصیف کند که تحت آن خرابی یا ناسازگار شدن منبع آنتروپی معلوم شود. روش‌های استفاده شده برای شناسایی شکست یا تخریب منبع باید گنجانده شود.

آزمون سلامت

به طور خاص‌تر، همه آزمون‌های سلامت منبع آنتروپی و توجیه آن‌ها باید مستند شود. این مستند شامل شرحی است از آزمون‌های سلامت، نرخ و شرایطی که تحت آن هر آزمون سلامت اجرا شده است (به طور مثال، در آغاز، به طور مداوم، یا بر اساس تقاضا)، نتایج مورد انتظار برای هر آزمون سلامت، و منطقی که نشان می‌دهد چرا هر آزمونی برای تشخیص یک یا چند شکست در منبع آنتروپی مناسب دانسته شده است.

پیوست ۶ واژگان اختصاری

واژه اختصاری	معنای انگلیسی	ترجمه فارسی
AES	Advanced Encryption Standard	استاندارد رمزگذاری پیشرفته
AGD	Administrative guidance document	سند راهنما
ANSI	American National Standards Institute	مؤسسه ملی استاندارد آمریکا
API	Application Programming Interface	واسط برنامه نویسی برنامه‌کاربردی
ASLR	Address Space Layout Randomization	آدرس چیدمان فضای تصادفی
CESG	CommunicationsElectronics Security Group	گروه امنیت ارتباطات الکترونیک
CMC	Certificate Management over CMS	مدیریت گواهی بر روی CMS
CMS	Cryptographic Message Syntax	نحو پیغام رمزنگاری
CN	Common Names	نام‌های متداول
CRL	Certificate Revocation List	فهرست ابطال گواهی
CSA	Computer Security Act	قانون امنیت کامپیوتر
DEP	Data Execution Prevention	ممانعت از اجرای داده
DES	Data Encryption Standard	استاندارد رمزگذاری داده
DHE	Diffie-Hellman Ephemeral	موقت دایف - هلمن
DNS	Domain Name System	سامانه نام دامنه
DRBG	Deterministic Random Bit Generator	تولید کننده بیت تصادفی قطعی
DSS	Digital Signature Standard	استاندارد امضای دیجیتال

DT	Date/Time Vector	بردار تاریخ یا زمان
DTLS	Datagram Transport Layer Security	امنیت لایه انتقال دیتاگرام
EAP	Extensible Authentication Protocol	پروتکل احراز هویت قابل توسعه
ECDHE	Elliptic Curve Diffie-Hellman Ephemeral	منحنی بیضوی دایفی - هلمن موقت
ECDSA	Elliptic Curve Digital Signature Algorithm	الگوریتم امضای دیجیتال منحنی بیضوی
EST	Enrollment over Secure Transport	نام نویسی بر روی انتقال امن
FIPS	Federal Information Processing Standards	استانداردهای پردازش اطلاعات فدرال
HMAC	Hash-based Message Authentication Code	کد احراز هویت پیام مبتنی بر چکیده‌ساز
HTTP	Hypertext Transfer Protocol	پروتکل انتقال فرامتن
HTTPS	Hypertext Transfer Protocol Secure	پروتکل انتقال فرامتن امن
IETF	Internet Engineering Task Force	نیروی اجرای عملیات مهندسی اینترنت
IP	Internet Protocol	پروتکل اینترنت
ISO	International Organization for Standardization	سازمان بین المللی استاندارد
IT	Information Technology	فناوری اطلاعات
ITSEF	Information Technology Security Evaluation Facility	افزارگان ارزیابی امنیت فناوری اطلاعات
KAT	Known Answer Tests	آزمون پاسخ معلوم
KEK	key encryption key	کلید رمزگذاری کلید
NFC	Near Field Communication	ارتباطات حوزه نزدیک
NIAP	National Information Assurance Partnership	انجمن تضمین اطلاعات ملی

NIST	National Institute of Standards and Technology	مؤسسه ملی استاندارد و فناوری
OCSP	Online Certificate Status Protocol	پروتکل وضعیت گواهی برخط
OID	Object Identifier	شناسه موجودیت غیرفعال
OMB	Office of Management and Budget	دفتر مدیریت و بودجه
OS	Operating System	سیستم‌عامل
PII	Personally Identifiable Information	اطلاعات قابل شناسایی شخصی
PKI	Public Key Infrastructure	زیرساخت کلید عمومی
PP	Protection Profile	پروفایل حفاظتی
RBG	Random Bit Generator	تولید کننده بیت تصادفی
RFC	Request for Comment	درخواست برای تفسیر
RNG	Random Number Generator	تولید کننده عدد تصادفی
RNGVS	Random Number Generator Validation System	سامانه اعتبارسنجی تولید کننده عدد تصادفی
SAN	Subject Alternative Name	نام جایگزین موجودیت فعال
SAR	Security Assurance Requirement	الزامات تضمین امنیت
SFR	Security Functional Requirement	الزامات کارکرد امنیت
SHA	Secure Hash Algorithm	الگوریتم چکیده‌ساز امن
S/MIME	Secure/Multipurpose Internet Mail Extensions	توسعه‌های پست اینترنتی چند منظوره یا امن
SIP	Session Initiation Protocol	پروتکل آغاز نشست
SWID	Software Identification	شناسایی نرم‌افزار

TLS	Transport Layer Security	امنیت لایه انتقال
URI	Uniform Resource Identifier	شناسه منبع یکپارچه
URL	Uniform Resource Locator	نشانی وب یا مکان یکنواخت منبع
USB	Universal Serial Bus	گذرگاه سریال فراگیر
VPN	Virtual Private Network	شبکه مجازی خصوصی
XCCDF	eXtensible Configuration Checklist Description Format	قالب توصیف فهرست پیکربندی قابل گسترش
XOR	Exclusive Or	اپراتور بولی (یای انحصاری)

پیوست ۷ مراجع

No.	Identifier	Title
1.	[CC]	Common Criteria for Information Technology Security Evaluation ▪ Part1: Introduction and General Model, CCMB201209001,Version ▪ 3.1 Revision 4, September 2012. ▪ Part 2: Security Functional Components, CCMB201209002, Version3.1 Revision 4, September 2012. ▪ Part 3: Security Assurance Components, CCMB201209003,Version3.1 Revision 4, September 2012
2.	[CEM]	Common Evaluation Methodology for Information Technology Security Evaluation Methodology, CCMB201209004, Version 3.1, Revision 4, September 2012.
3.	[CESG]	CESG End User Devices Security and Configuration Guidance
4.	[CSA]	Computer Security Act of 1987, H.R. 145, June 11, 1987.
5.	[OMB]	Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, OMB M0619, July 12, 2006.