INSO
16300-1
1st. Edition
May.2013

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

استاندارد ملی ایران
۱-۱۶۳۰۰
چاپ اول
اردیبهشت ۱۳۹۲

فناوری اطلاعات - اتصال متقابل سامانه‌های باز- چارچوب‌های کاری امنیتی برای سامانه‌های باز: مرور کلی

Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview

ICS: 35.100.01

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

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

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

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

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

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

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

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- اتصال متقابل سامانه‌های باز - چارچوب‌های کاری امنیتی برای سامانه‌های باز: مرور کلی»

رئیس:	**سمت و/یا نمایندگی**
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر - نرم افزار)	کارشناس سازمان فناوری اطلاعات
دبیر:	
میر اسکندری، سید محمدرضا (لیسانس مهندسی کامپیوتر - نرم افزار)	مدیرکل خدمات ارزش افزوده سازمان فناوری اطلاعات
اعضا: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (کارشناسی مهندسی برق)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
قسمتی، سیمین (کارشناسی ارشد فناوری اطلاعات)	کارشناس سازمان فناوری اطلاعات
جمیل پناه، ناصر (فوق لیسانس مدیریت)	کارشناس سازمان فناوری اطلاعات
حسینی نژاد راهی، بابک (لیسانس علوم کامپیوتر)	نماینده دانشگاه علم و صنعت ایران
سعیدی، عذراء (فوق لیسانس مهندسی مخابرات)	کارشناس سازمان فناوری اطلاعات
عبداللهی ازگمی، محمد (دکترای مهندسی کامپیوتر – نرم‌افزار)	استادیار دانشگاه علم و صنعت ایران
عسکرزاده، مجید (کارشناسی‌ارشد مهندسی کامپیوتر)	کارشناس ارشد پژوهشگاه ارتباطات و فناوری اطلاعات

فولادیان، مجید (کارشناسی ارشد مهندسی مخابرات)	مشاور سازمان فناوری اطلاعات ایران
کبیری، پیمان (دکترای مهندسی کامپیوتر)	استادیار دانشگاه علم و صنعت ایران
میرزایی رضایی، طیبه (فوق لیسانس فیزیک)	رئیس اداره تدوین استاندارد ها و نظارت بر فرآیند سرویس‌ها سازمان فناوری اطلاعات

فهرست مندرجات

عنوان **صفحه**

آشنایی با سازمان ملی استاندارد ب
کمیسیون فنی تدوین استاندارد ج
پیش‌گفتار ز
مقدمه ح
۱ هدف و دامنه کاربرد ۱
۲ مراجع الزامی ۲
۳ اصطلاحات و تعاریف ۲
۳-۱ تعاریف مربوط به مدل مرجع پایه ۲
۳-۲ تعاریف مربوط به معماری امنیتی ۲
۳-۳ تعاریف افزوده ۳
۴ کوته‌نوشت‌ها ۹
۵ نشانه‌گذاری ۹
۶ سازمان ۹
۶-۱ قسمت ۱ – مرور کلی ۹
۶-۲ قسمت ۲ – احراز هویت ۱۰
۶-۳ قسمت ۳ – کنترل دسترسی ۱۰
۶-۴ قسمت ۴ – انکارناپذیری ۱۱
۶-۵ قسمت ۵ – محرمانگی ۱۱
۶-۶ قسمت ۶ – یکپارچگی ۱۲
۶-۷ قسمت ۷ – ممیزی و هشدارهای امنیتی ۱۲
۶-۸ مدیریت کلید ۱۳
۷ مفاهیم عمومی ۱۳
۷-۱ اطلاعات امنیتی ۱۳
۷-۲ دامنه‌ی امنیتی ۱۴
۷-۳ ملاحظات خط مشی امنیتی برای خدمات امنیتی خاص ۱۷
۷-۴ هستارهای قابل اعتماد ۱۸
۷-۵ اعتماد ۱۹
۷-۶ طرف‌های سوم قابل اعتماد ۱۹
۸ اطلاعات امنیتی عمومی ۲۰

۸-۱ برچسب‌های امنیتی ۲۰
۸-۲ مقادیر وارسی رمزنگاشتی ۲۰
۸-۳ گواهی‌های امنیت ۲۲
۸-۴ نشانه‌های امنیتی ۲۵
۹ تسهیلات امنیتی کلی ۲۵
۹-۱ تسهیلات مرتبط با مدیریت ۲۵
۹-۲ تسهیلات مربوط به عملیات ۲۷
۱۰ برهم‌کنش بین سازوکارهای امنیتی ۲۸
۱۱ دسترس‌پذیری و انکار خدمت ۲۹
۱۲ سایر الزامات ۳۰
پیوست الف: مثال‌هایی از سازوکارهای محافظتی برای گواهی‌های امنیتی (اطلاعاتی) ۳۱
الف-۱ محافظت با استفاده از یک خدمت امنیتی ارتباطات در OSI ۳۱
الف-۲ محافظت با استفاده از یک پارامتر درونی گواهی‌های امنیتی ۳۱
الف-۳ محافظت از پارامترهای درونی و بیرونی در حال انتقال ۳۳
پیوست ب: کتابنامه (اطلاعاتی) ۳۶

پیش‌گفتار

استاندارد «فناوری اطلاعات - اتصال متقابل سامانه‌های باز - چارچوب‌های کاری امنیتی برای سامانه‌های باز: مرور کلی» که پیش‌نویس آن درکمیسیون‌های مربوط توسط سازمان فناوری اطلاعات تهیه و تدوین شده و در دویست و بیست و یکمین اجلاسیه کمیته‌ی ملی استاندارد رایانه و فناوری داده مورخ ۱۳۹۱/۹/۲۶ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات سازمان ملی استاندارد ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

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

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

ISO/IEC 10181-1:1996 , Information technology - Open Systems Interconnection - Security frameworks for open systems: Overview.

مقدمه

کاربردهای زیادی برای محافظت در مقابل تهدیدات علیه ارتباط اطلاعات نیازمند امنیت هستند. برخی از تهدیدات شناخته شده معمول، به همراه خدمات و سازوکارهای امنیتی[1] که برای محافظت در مقابل آن‌ها قابل استفاده هستند در توصیه‌نامه X.800 شورای بین‌المللی تلگراف و تلفن (CCITT)[2] | ISO 7498-2 شرح داده شده‌اند.

این استاندارد ملی یک چارچوب کاری را تعریف می‌کند که در آن خدمات امنیتی برای سامانه‌های باز مشخص شده‌اند.

1 - Security mechanisms
2 - Comité Consultatif International Téléphonique et Télégraphique

فناوری اطلاعات - اتصال متقابل سامانه‌های باز- چارچوب‌های کاری امنیتی برای سامانه‌های باز: مرور کلی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین مشخصات چارچوب‌های کاری امنیتی[1] است که به کاربرد خدمات امنیتی در محیط یک سامانه باز توجه دارند. جایی که عبارت *سامانه‌ی باز* شامل حوزه‌هایی از قبیل پایگاه داده، کاربردهای توزیع‌شده، پردازش توزیع‌شده باز (ODP)[2] و اتصال متقابل سامانه‌های باز (OSI)[3] می‌شود. چارچوب‌های کاری امنیتی به تعریف ابزارهای فراهم‌کننده‌ی محافظت برای سامانه‌ها و اشیاء درون سامانه‌ها و روابط بین سامانه‌ها می‌پردازند. چارچوب‌های کاری امنیتی به روشگان[4] و سازوکارهای ایجاد سامانه‌ها توجه‌ای ندارند.

چارچوب‌های کاری امنیتی عناصر داده‌ای و دنباله‌هایی از عملیات (اما نه عناصر پروتکل) را مورد توجه قرار می‌دهند که برای به‌دست آوردن خدمات امنیتی خاصی مورد استفاده قرار می‌گیرند. این سرویس‌های امنیتی ممکن است برای هستارهای ارتباطی[5] سامانه‌ها و یا داده‌های انتقال یافته بین سامانه‌ها و داده‌های مدیریت شده به‌وسیله‌ی سامانه‌ها مورد استفاده قرار گیرند.

چارچوب‌های کاری امنیتی مبنایی برای استانداردسازی بیشتر را با فراهم کردن واژگان سازگار و تعاریف مربوط به واسطهای خدمات انتزاعی کلی برای الزامات خاص امنیتی، ایجاد می‌کنند. چارچوب‌ها علاوه بر این سازوکارهایی را دسته‌بندی می‌کنند که می‌توان برای دسترسی به آن الزامات مورد استفاده قرار گیرند.

یک خدمت امنیتی اغلب به خدمات امنیتی دیگر وابسته است که این امر جداسازی یک قسمت از امنیت را از سایر اجزا دشوار می‌سازد. چارچوب‌های کاری امنیتی، خدمات امنیتی خاصی را مورد نظر قرار داده و محدوده‌ی سازوکارهای مورد استفاده برای ایجاد آن خدمات را مشخص و وابستگی داخلی بین خدمات و سازوکارها را تعیین می‌کنند. توضیح این سازوکارها ممکن است مستلزم اتکا به خدمت امنیتی متفاوتی باشد که در این صورت چارچوب‌های کاری امنیتی اتکای یک خدمت را به دیگری توصیف می‌کنند.

این بخش از چارچوب کاری امنیتی:

- سازمان‌دهی چارچوب‌های کاری امنیتی را توصیف می‌کند؛
- مفاهیم امنیتی مورد نیاز در بیش از یک بخش از چارچوب‌های کاری امنیتی را تعریف می‌کند؛
- روابط درونی خدمات و سازوکارهای شناسایی شده در سایر بخش‌های چارچوب‌ها را توصیف می‌کند.

---

1 - Security frameworks
2 - Open Distributed Processing
3 - Open System Interconnection
4 - Methodology
5 - Communication entities

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آن‌ها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد ملی ایران محسوب می‌شود.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدید نظرهای بعدی آن مورد نظر این استاندارد ملی نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره تاریخ تجدید نظر و اصلاحیه‌های بعدی آن‌ها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-l: 1994, Information technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.

2-1 CCITT Recommendation X.800 (1991), Security architecture for Open Systems Interconnection for CCITT applications.

2-1 ISO 7498-2:1989, Information Processs systems - Open Systems Interconnection - Basic Reference Mode –Part 2: Security Architecture**.**

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به کار می‌رود:

تعاریف زیر در این قسمت یا قسمت‌های دیگری از چارچوب‌های کاری امنیتی مورد استفاده قرار می‌گیرند.

۳-۱ تعاریف مربوط به مدل مرجع پایه

این استاندارد ملی از اصطلاحات زیر استفاده می‌کند که در توصیه‌نامه ISO/IEC 7498-1|X.200 اتحادیه بین‌المللی مخابرات (ITU)[1] تعریف شده‌اند.

- (N)-لایه[2]؛
- (N)-هستار[3]؛
- (N)-واحد داده‌ای پروتکل[4]؛
- فرآیند کاربردی[5]؛
- سامانه‌ی باز واقعی؛
- سامانه‌ی واقعی.

۳-۱-۱ تعاریف مربوط به معماری امنیتی

این استاندارد ملی از عبارات زیر استفاده می‌کند که در توصیه‌نامه ISO 7498-2|CCITT X.800 تعریف شده‌اند.

- کنترل دسترسی[6]؛

1 - International Telecommunication Union
2 - (N)-layer
3 - (N)-entity (منظور هستار لایه N است)
4 - (N)-protocol-data-unit (منظور واحد داده‌ای پروتکل لایه N است)
5 - Application process
6 - Access control

- دسترس‌پذیری[1]؛
- متن رمزشده[2]؛
- مقدار وارسی رمزنگاشتي[3]؛
- رمزگشایی[4]؛
- انکار خدمت[5]؛
- امضای دیجیتالی[6]؛
- رمزگذاری[7]؛
- تهدید نفوذگر داخلی[8]؛
- کلید؛
- مدیریت کلید[9]؛
- متن ساده[10]؛
- تهدید نفوذگر خارجي[11]؛
- ممیزی امنیتی[12]؛
- برچسب امنیتی[13]؛
- خط مشی امنیتی[14]؛
- حساسیت[15]؛
- تهدید[16].

۳-۲ تعاریف افزوده

برای تحقق اهداف این استاندارد از تعاریف زیر استفاده می‌شود.

۳-۲-۱

الگوریتم رمزنگاشتی نامتقارن

الگوریتمی برای رمزگذاری (رمزنگاری) یا رمزگشایی که در آن کلیدهای مورد استفاده برای رمزگذاری و رمزگشایی با یکدیگر متفاوتند.

---

1 - Availability
2 - Ciphertext
3 - Cryptographic check value
4 - Decipherment
5 - Denial of service
6 - Digital signatue
7 - Encipherment
8 - Insider threat
9 - Key management
10 - Plaintext
11 - Outsider threat
12 - Security audit
13 - Security label
14 - Security policy
15 - Sensitivity
16 - Threat

یادآوری- در برخی الگوریتم‌های رمزنگاشتی نامتقارن، رمزگشایی یک متن رمزشده و یا ایجاد یک امضای دیجیتالی نیازمند استفاده از بیش از یک کلید خصوصی[1] است.

۲-۲-۳

مرجع گواهی[2]

یک هستار مورد اعتماد[3] (در زمینه‌ی یک خط مشی امنیتی) برای ایجاد گواهی‌های امنیتی که شامل یک یا چند رده از داده‌های مرتبط با امنیت است.

۳-۲-۳

هستار قابل اعتماد مشروط[4]

هستاری که در زمینه‌ی خط مشی امنیتی قابل اعتماد بوده اما نمی‌تواند از خط مشی امنیتی بدون آنکه شناسایی شود، تخطی کند.

۴-۲-۳

زنجیره‌سازی رمزنگاشتی[5]

یک نوع استفاده از یک الگوریتم رمزنگاشتی است که در آن تبدیلات انجام شده به‌وسیله‌ی الگوریتم به مقادیر ورودی‌ها و خروجی‌های قبلی وابسته است.

۵-۲-۳

اثر انگشت رقمی[6]

خصوصیتی از یک قلم داده، مانند یک مقدار وارسی رمزنگاشتی شده یا نتیجه‌ی اجرای یک تابع درهم‌سازی یک سویه بر روی داده‌ها، که برای آن واحد داده به اندازه‌ی کافی خاص بوده به طوری که واحد داده‌ی دیگری را نمی‌توان یافت که همان خصوصیت‌ها را داشته باشد.

۶-۲-۳

شناسه متمایزکننده[7]

داده‌هایی که یک هستار را به طور یکتا تمیز می‌دهند.

---

1 - Private key
2 - Certification authority
3 - Trusted
4 - Conditionally trusted entity
5 - Cryptographic chaining
6 - Digital fingerprint
7 - Distinguishing identifier

۷-۲-۳

تابع درهم‌سازی[1]

یک تابع (ریاضی) که انجام آن ساده بوده، اما با دانستن یک نتیجه از آن، یافتن هر کدام از مقداری که منجر به آن نتیجه شده است از نظر محاسباتی غیرممکن است.

۸-۲-۳

تابع یک سویه[2]

یک تابع ریاضی است که انجام آن ساده بوده اما با دانستن یک نتیجه از آن، یافتن مقداری که منجر به آن نتیجه شده از نظر محاسباتی غیرممکن است.

۹-۲-۳

تابع درهم‌سازی یک سویه

یک تابع ریاضی که هم یک تابع یک سویه و هم یک تابع درهم‌سازی است.

۱۰-۲-۳

کلید خصوصی[3]

یک کلید که در یک الگوریتم رمزنگاشتی نامتقارن مورد استفاده قرار می‌گیرد که دانستن آن (به طور معمول به تنها یک هستار) محدود شده است.

۱۱-۲-۳

کلید عمومی[4]

کلیدی که در یک الگوریتم رمزنگاشتی نامتقارن مورد استفاده قرار می‌گیرد و می‌توان آن را در دسترس عموم قرار داد.

۱۲-۲-۳

گواهی لغو[5]

یک گواهی امنیتی که به‌وسیله‌ی یک هستار مرجع صادر شده و مشخص می‌کند که یک گواهی امنیتی خاص ملغی شده است.

---

1 - Hash function
2 - One-way function
3 - Private key
4 - Public key
5 - Revocation certificate

۱۳-۲-۳

گواهی فهرست لغو[1]

یک گواهی امنیتی که مشخص‌کننده‌ی فهرستی از گواهی‌های امنیتی ملغی شده است.

۱۴-۲-۳

مُهر[2]

یک مقدار وارسی رمزنگاشتی که از یکپارچگی[3] پشتیبانی کرده اما در برابر جعل شدن به‌وسیله‌ی یک دریافت کننده، محافظتی نخواهد داشت (یعنی انکارناپذیری را فراهم نمی‌کند). هنگامی که یک مُهر به یک عنصر داده‌ای هم‌بسته می‌شود، گفته می‌شود که آن عنصر داده‌ای مُهر شده است.

یادآوری- هر چند که یک مُهر خود به تنهایی انکارناپذیری را فراهم نمی‌کند، برخی سازوکارهای انکارناپذیری، از یکپارچگی فراهم شده به‌وسیله‌ی مُهرها استفاده می‌کنند، به عنوان مثال برای محافظت از ارتباطات با طرف سوم مورد اعتماد.

۱۵-۲-۳

کلید سرّی[4]

کلیدی که در یک الگوریتم رمزنگاشتی متقارن مورد استفاده قرار می‌گیرد. داشتن یک کلید سرّی محدود است (به طور معمول به دو هستار).

۱۶-۲-۳

مدیر امنیتی[5]

شخصی که موظف است یک یا چند جزء از خط مشی امنیتی را تعریف و یا اجرا کند.

۱۷-۲-۳

مرجع امنیتی[6]

هستاری که موظف است یک خط مشی امنیتی را تعریف، پیاده‌سازی و اجرا کند.

1 - Revocation list certificate
2 - Seal
3 - Integrity
4 - Secret key
5 - Security administrator
6 - Security authority

۳-۲-۱۸

گواهی امنیتی

مجموعه‌ای از داده‌های مرتبط با امنیت که به‌وسیله‌ی یک مرجع امنیتی یا یک طرف سوم قابل اعتماد به همراه اطلاعات امنیتی مورد استفاده برای فراهم‌سازی خدمات یکپارچگی داده‌ها و احراز هویت مبدأ داده‌ها، صادر می‌شود.

یادآوری- تمامی گواهی‌ها، گواهی‌های امنیتی هستند (به تعاریف موجود مرتبط در استاندارد ISO 7498-2 مراجعه کنید). از عبارت گواهی امنیتی برای این‌که با واژگان موجود در توصیه‌نامه ITU-T X509 | ISO/IEC 9594-1 تعارض نداشته باشد، استفاده می‌شود.

۳-۲-۱۹

زنجیره‌ی گواهی امنیتی

دنباله‌ای پشت سر هم از گواهی‌های امنیتی بوده که در آن اولین گواهی امنیتی شامل اطلاعات مرتبط با امنیت بوده و هر گواهی امنیتی بعدی شامل اطلاعات امنیتی است که می‌تواند برای درستی‌سنجی[1] گواهی‌های امنیتی پیشین مورد استفاده باشد.

۳-۲-۲۰

دامنه‌ی امنیتی

مجموعه‌ای از عناصر، یک خط مشی امنیتی، یک مرجع امنیتی و مجموعه‌ای از فعالیت‌های امنیتی است که در آن فعالیت‌های هر عنصر منوط به خط مشی امنیتی بوده و خط مشی امنیتی به‌وسیله‌ی مرجع امنیتی مدیریت می‌شود.

۳-۲-۲۱

مرجع دامنه‌ی امنیتی

یک مرجع امنیتی که مسئول پیاده‌سازی یک خط مشی امنیتی برای یک دامنه‌ی امنیتی است.

۳-۲-۲۲

اطلاعات امنیتی

اطلاعاتی که برای پیاده‌سازی خدمات امنیتی مورد نیاز هستند.

۳-۲-۲۳

بازیابی امنیتی[2]

فعالیت‌ها یا روال‌هایی که در زمان تشخیص یا مشکوک شدن به یک تخلف امنیتی باید انجام شوند.

---

1 - Verification
2 - Security recovery

۲۴-۲-۳

قواعد برهم‌کنش امن[1]

قواعد خط مشی امنیتی که برهم‌کنش بین دامنه‌های امنیتی را نظم می‌بخشد.

۲۵-۲-۳

قواعد خط مشی امنیتی

بازنمایی یک خط مشی امنیتی برای یک دامنه‌ی امنیتی در یک سامانه‌ی واقعی است.

۲۶-۲-۳

نشانه‌ی امنیتی[2]

مجموعه‌ای از داده‌ها که به‌وسیله‌ی یک یا چند خدمت امنیتی محافظت می‌شوند. به همراه اطلاعات امنیتی مورد استفاده در فراهم‌سازی آن خدمات امنیتی، که بین هستارهای ارتباطی منتقل می‌شود.

۲۷-۲-۳

الگوریتم رمزنگاشتی متقارن

یک الگوریتم برای اجرای رمزگذاری یا الگوریتمی برای اجرای رمزگشایی متناظر با آن که در آن برای رمزگذاری و رمزگشایی از کلیدهای یکسان استفاده می‌شود.

۲۸-۲-۳

اعتماد[3]

گفته می‌شود که هستار X به هستار Y برای انجام مجموعه‌ای از فعالیت‌ها *اعتماد دارد* اگر و تنها اگر هستار X به هستار Y رفتارکننده به روشی خاص با در نظر گرفتن فعالیت‌ها، اتکا داشته باشد.

۲۹-۲-۳

هستار غیرقابل اعتماد[4]

یک هستار که می‌تواند با انجام دادن عملیاتی که نباید انجام دهد یا با انجام ندادن عملیاتی که باید انجام دهد، از یک خط مشی امنیتی تخطی کند.

1 - Secure interaction rules
2 - Security token
3 - Trust
4 - Untrusted entity

۳۰-۲-۳

طرف سوم قابل اعتماد[1]

یک مرجع امنیتی یا عامل آن که برای برخی فعالیت‌های مرتبط با امنیت (در زمینه یک خط مشی امنیتی) مورد اعتماد است.

۳۱-۲-۳

هستار قابل اعتماد بدون شرط[2]

یک هستار قابل اعتماد که بدون آنکه شناسایی شود می‌تواند از خط مشی امنیتی تخطی کند.

۴ کوته‌نوشت‌ها

برای تحقق اهداف این استاندارد ملی، از کوته‌نوشت‌های زیر استفاده می‌شود:

اطلاعات کنترل دسترسی	Access Control Information	ACI
اتصال متقابل سامانه‌های باز	Open Systems Interconnection	OSI
پردازش توزیع‌شده‌ی باز	Open Distributed Processing	ODP
اطلاعات امنیتی	Security Information	SI
طرف سوم قابل اعتماد	Trusted Third Party	TTP

۵ نشانه‌گذاری

نشانه‌گذاری لایه همان است که در توصیه‌نامه ITU-T X.200 | ISO/IEC 7498-1 تعریف شده است.

عبارت خدمت برای ارجاع به یک خدمت امنیتی مورد استفاده قرار می‌گیرد مگر آنکه خلاف آن ثابت شود.

عبارت گواهی برای ارجاع به یک گواهی امنیتی مورد استفاده قرار می‌گیرد مگر آنکه خلاف آن ثابت شود.

۶ سازمان[3]

چارچوب‌های کاری امنیتی جزئی از استاندارد ملی چند جزئی (ISO/IEC 10181) و دنباله‌ای از توصیه‌های ITU هستند. چارچوب‌های کاری امنیتی در زیر توضیح داده می‌شوند. چارچوب‌های کاری امنیتی بیشتری ممکن است در آینده تعریف شوند. چارچوب مدیریت کلید جزئی از ISO/IEC 10181 نیست اما زمینه‌ی یکسانی داشته و برای کامل بودن، توضیحات آن را نیز شامل می‌شود.

۱-۶ قسمت ۱ - مرور کلی

به بند ۱ مراجعه کنید.

1 - Trusted third party
2 - Unconditionally trusted entity
3 - Organization

۶-۲ قسمت ۲ - احراز هویت

این چارچوب تمامی جنبه‌های احراز هویت، از جمله مواردی که بر سامانه‌های باز اعمال می‌شوند، روابط احراز هویت با سایر کارکردهای امنیتی[1]، از جمله کنترل دسترسی و نیز الزامات مدیریتی برای احراز هویت را توصیف می‌کند.

این چارچوب:

الف- مفاهیم پایه‌ی احراز هویت را تعریف می‌کند؛

ب- انواع رده‌های ممکن از سازوکارهای احراز هویت را مشخص می‌کند؛

پ- خدمات امنیتی مورد استفاده برای انواع رده های ممکن سازوکارهای احراز هویت را تعیین می‌کند؛

ت- الزامات کارکردی برای پروتکل‌ها را به منظور پشتیبانی از انواع رده‌های ممکن سازوکارهای احراز هویت را تعیین می‌کند؛ و

ث- الزامات کلی مدیریتی را برای احراز هویت مشخص می‌کند.

چارچوب کاری احراز هویت جایگاهی در بالای سلسله‌مراتب استانداردهای احراز هویت دارد که مفاهیم، فهرست واژگان و یک طبقه‌بندی برای روش‌های احراز هویت فراهم می‌کند. پس از آن، استانداردهایی مانند ISO/IEC 9798 (سازوکارهای احراز هویت هستار) مجموعه‌ای خاص از این روش‌ها را با جزئیات بیشتری فراهم می‌کنند. در نهایت، در انتهای سلسله‌مراتب، استانداردهایی مانند توصیه‌نامه ITU-T Rec X.509 | ISO/IEC 9594-8 (چارچوب کاری احراز هویت فهرست راهنما[2]) از این مفاهیم و روش‌ها در زمینه‌ی یک کاربرد خاص یا نیاز خاص استفاده می‌کنند.

چارچوب کاری احراز هویت مدلی از احراز هویت، تعدادی از گام‌هایی که فعالیت‌های احراز هویت را می‌توان به آن‌ها دسته‌بندی کرد، استفاده از یک طرف سوم قابل اعتماد، استفاده از گواهی‌های احراز هویت برای تبادل اطلاعات احراز هویت، یک خدمت کلی احراز هویت مبتنی بر این گام‌ها و حداقل پنج رده از سازوکارهای احراز هویت را که خدمت کلی احراز هویت را فراهم می‌سازند، توصیف می‌کند. این سازوکارها شامل محافظت در برابر افشای اطلاعات احراز هویت و بازپخش[3] بر روی همان احراز کننده‌ی هویت[4] یا احراز کننده‌ای دیگر می‌شود.

۶-۳ قسمت ۳ - کنترل دسترسی

این چارچوب تمامی جنبه‌های کنترل دسترسی (برای مثال، از جمله دسترسی‌های کاربر به فرآیند، کاربر به داده، فرآیند به فرآیند، فرآیند به داده) در سامانه‌های باز، ارتباط با سایر کارکردهای امنیتی از جمله احراز هویت و ممیزی، و الزامات مدیریتی برای کنترل دسترسی را توصیف می‌کند.

این چارچوب:

الف- مفاهیم پایه‌ی کنترل دسترسی را تعریف می‌کند؛

1 - Security Functions
2 - Directory
3 - Replay
4 - Authenticator

ب- روشی را نشان می‌دهد که با آن مفاهیم پایه‌ی کنترل دسترسی برای پشتیبانی از برخی خدمات و سازوکارهای شناخته شده‌ی کنترل دسترسی، تخصصی می‌شوند؛
پ- این خدمات و سازوکارهای کنترل دسترسی متناظر را تعریف می‌کند؛
ت- الزامات کارکردی پروتکل‌ها جهت پشتیبانی از این خدمات و سازوکارهای کنترل دسترسی را شناسایی می‌کند؛
ث- الزامات مدیریتی برای پشتیبانی از این خدمات و سازوکارهای کنترل دسترسی را شناسایی می‌کند؛ و
ج- برهم‌کنش بین خدمات و سازوکارهای کنترل دسترسی با سایر خدمات و سازوکارها را مورد توجه قرار می‌دهد.

این چارچوب کاری امنیتی، مدلی از کنترل دسترسی، تعدادی از گام‌هایی که فعالیت‌های کنترل دسترسی را می‌توان به آن‌ها دسته‌بندی کرد، یک خدمت کلی کنترل دسترسی مبتنی بر این گام‌ها و حداقل سه رده از سازوکارهای امنیتی که این خدمت کلی کنترل دسترسی را فراهم می‌کنند را توصیف می‌کند. این سازوکارها عبارتند از فهرست‌های کنترل دسترسی، قابلیت‌ها[1] و برچسب‌ها.

۶-۴ قسمت ۴ - انکارناپذیری

این چارچوب مفاهیم خدمات انکارناپذیری را که در توصیه‌نامه CCITT X.800 | ISO 7498-2 تعریف شده‌اند اصلاح و گسترش داده و چارچوبی برای توسعه و فراهم‌سازی این خدمات ارائه می‌کند.

این چارچوب:

الف- مفاهیم پایه‌ی انکارناپذیری را تعریف می‌کند؛
ب- خدمات انکارناپذیری کلی را تعریف می‌کند؛
پ- سازوکارهای ممکن برای فراهم کردن خدمات انکارناپذیری را شناسایی می‌کند؛ و
ت- الزامات مدیریتی کلی برای خدمات و سازوکارهای انکارناپذیری را شناسایی می‌کند.

۶-۵ قسمت ۵ - محرمانگی

هدف خدمت محرمانگی محافظت از اطلاعات در برابر افشای غیرمجاز است. این چارچوب محرمانگی اطلاعات را در بازیابی، انتقال و مدیریت آن‌ها مورد توجه قرار می‌دهد.

این چارچوب:

الف- مفاهیم پایه‌ی محرمانگی را تعریف می‌کند؛
ب- رده‌های ممکن سازوکارهای محرمانگی را مشخص می‌کند؛
پ- تسهیلات هر رده از سازوکارهای محرمانگی را تعریف می‌کند؛
ت- مدیریت مورد نیاز برای پشتیبانی از رده‌های سازوکارهای محرمانگی را مشخص می‌کند؛ و
ث- برهم‌کنش سازوکارهای محرمانگی و خدمات پشتیبان با سایر خدمات و سازوکارها را مورد توجه قرار می‌دهد.

1 - Capabilities

برخی از روال‌های توضیح داده شده در این چارچوب کاری امنیتی به‌وسیله‌ی کاربرد رمزنگاری به محرمانگی دست می‌یابند. استفاده از این چارچوب وابسته به استفاده از رمزنگاری خاصی یا الگوریتم‌های دیگر نیست. اگرچه رده‌های خاصی از سازوکارهای محرمانگی ممکن است به برخی از خصوصیت‌های الگوریتم‌های خاصی وابسته باشند.

۶-۶ قسمت ۶ - یکپارچگی

این ویژگی که داده‌ها به‌وسیله‌ی یک رفتار غیرمجاز تغییر نیافته‌اند و یا از بین نرفته‌اند را یکپارچگی گویند. این چارچوب، یکپارچگی داده‌ها را در بازیابی، انتقال و مدیریت مورد توجه قرار می‌دهد.

این چارچوب:

الف- مفاهیم پایه‌ی یکپارچگی را تعریف می‌کند؛

ب- رده‌های ممکن برای سازوکارهای یکپارچگی را شناسایی می‌کند؛

پ- تسهیلات هر رده از سازوکارهای یکپارچگی را تعریف می‌کند؛

ت- مدیریت مورد نیاز برای پشتیبانی از رده‌های سازوکارهای یکپارچگی را شناسایی می‌کند؛ و

ث- برهم‌کنش سازوکارهای یکپارچگی و خدمات پشتیبان با سایر خدمات و سازوکارها را مورد توجه قرار می‌دهد.

برخی از روال‌های توضیح داده شده در این چارچوب کاری امنیتی با استفاده از روش‌های رمزنگاری به یکپارچگی دست می‌یابند. استفاده از این چارچوب وابسته به استفاده از رمزنگاری یا الگوریتم‌های دیگر نیست. اگرچه رده‌های خاصی از سازوکارهای یکپارچگی ممکن است به برخی از خصوصیت‌های الگوریتم‌های خاصی وابسته باشند.

یکپارچگی مورد نظر این چارچوب به‌وسیله‌ی ثبات[1] مقدار داده و نه ثبات اطلاعاتی که به‌وسیله‌ی آن داده نمایش داده شده است تعریف می‌شود. سایر اشکال تغییر ناپذیری در این تعریف جای نمی‌گیرند.

۶-۷ قسمت ۷ - ممیزی و هشدارهای امنیتی

این چارچوب:

الف- مفاهیم پایه‌ی ممیزی و هشدارهای امنیتی را تعریف می‌کند؛

ب- طرحی کلی برای ممیزی و هشدارهای امنیتی را فراهم می‌کند؛ و

پ- برهم‌کنش خدمات ممیزی و هشدارهای امنیتی با سایر خدمات امنیتی را مورد توجه قرار می‌دهد.

همانند سایر خدمات امنیتی، یک ممیزی امنیتی تنها می‌تواند در زمینه‌ی یک خط مشی امنیتی تعریف شده فراهم شود. خط مشی امنیتی به‌وسیله‌ی مراجع امنیتی درون دامنه‌ی امنیتی‌اش تعریف می‌شود. هر استانداردی که مشخص کننده‌ی سازوکارهایی بر مبنای این چارچوب باشد باید قابلیت پشتیبانی از خط مشی های امنیتی متفاوت را داشته باشد.

---

1 - Constancy

۸-۶ مدیریت کلید

چارچوب مدیریت کلید، قسمت ۱ از استاندارد ISO/IEC 11770، رابطه‌ی ویژه‌ای با سایر چارچوب‌های کاری امنیتی که کارکردهایشان به طور مستقیم به خدمات امنیتی مشخص شده در توصیه‌نامه CCITT X.800| ISO 7498-2 مربوط نمی‌شوند، دارد. این کارکردها در هر محیط فناوری اطلاعاتی که رمزگذاری و امضای دیجیتالی در آن‌ها قابل استفاده‌اند، قابل اجرا هستند.

این چارچوب:

الف- اهداف مدیریت کلید را مشخص می‌کند؛

ب- طرح‌های کلی که مدیریت کلید بر آن‌ها استوار است را توصیف می‌کند؛

پ- مفاهیم پایه‌ی مدیریت کلید که برای تمامی قسمت‌های این استاندارد چند قسمتی عمومیت دارد، تعریف می‌کند؛

ت- خدمات مدیریت کلید را تعریف می‌کند؛

ث- خصوصیت‌های سازوکارهای مدیریت کلید را شناسایی می‌کند؛

ج- نیازمندی‌های مدیریت ابزارهای کلیددهی را در طول حیاتشان مشخص می‌کند؛

چ- چارچوبی برای مدیریت ابزارهای کلیددهی را در طول حیاتشان معرفی کرده و توصیف می‌کند.

۷ مفاهیم عمومی

برخی از مفاهیم در بیش از یک قسمت از چارچوب‌های کاری امنیتی مورد نیاز هستند. این استاندارد این مفاهیم را برای استفاده در بقیه قسمت‌های این استاندارد تعریف می‌کند.

۷-۱ اطلاعات امنیتی

اطلاعات امنیتی (SI)[1]، اطلاعات مورد نیاز برای پیاده‌سازی خدمات امنیتی است. نمونه‌هایی از اطلاعات امنیتی عبارتند از:

- قواعد خط مشي امنیتی؛
- اطلاعاتی برای تحقق یافتن خدمات امنیتی خاص از جمله اطلاعات احراز هویت (AI)[2] و اطلاعات کنترل دسترسی (ACI)؛ و
- اطلاعات مرتبط با سازوکارهای امنیتی از جمله برچسب‌های امنیتی، مقادیر وارسی رمزنگاشتي، گواهی‌های امنیتی و نشانه‌های امنیتی.

انواع اطلاعات امنیتی که برای بیش از یک چارچوب کاری امنیتی عمومیت دارد در بند ۸ مورد بحث و بررسی قرار می‌گیرند.

1 - Security Information (SI)
2 - Authorization Information (AI)

۷-۲ دامنه‌ی امنیتی

یک دامنه‌ی امنیتی مجموعه‌ای از عناصر تحت یک خط مشی امنیتی اعمال شده به‌وسیله‌ی یک مرجع امنیتی برای برخی عملیات امنیتی خاص است. فعالیت‌های یک دامنه‌ی امنیتی ممکن است شامل یک یا چند عنصر از دامنه‌ی امنیتی و به احتمال عناصری از سایر دامنه‌های امنیتی باشد.

مثال‌هایی از این گونه فعالیت‌ها عبارتند از:

- دسترسی به عناصر؛
- برقراری یا استفاده از اتصالات لایه (N) در OSI؛
- عملیات مرتبط با یک کارکرد مدیریتی خاص؛
- عملیات انکارناپذیری شامل یک ثبت‌کننده.

یک فعالیت ممکن است مرتبط با امنیت باشد حتی اگر موضوع سازوکارهایی که می‌توانند یک خط مشی دلخواه را با توجه به کارکرد آن اعمال کنند ، نباشد. به خصوص فعالیت‌هایی که نمی‌توان از وقوع آن‌ها در هر گروهی از عناصر جلوگیری کرد، می‌توانند مرتبط با امنیت بوده و ممکن است در آینده مورد توجه سازوکارهای کنترل کننده قرار گیرند.

مثال‌هایی از عناصر یک دامنه‌ی امنیتی در یک محیط سامانه‌های باز عبارتند از: عناصر منطقی و فیزیکی مانند سیستم‌های باز واقعی، فرآیندهای کاربردی، (N)-هستار، (N)-واحدهای داده‌ای پروتکل، رله‌ها و کاربران سامانه‌های باز واقعی.گاهی کاربران باید از سایر عناصر یک دامنه‌ی امنیتی تمیز داده شوند. در این مواقع برای تشخیص عناصر غیر انسانی از عبارت اشیاء داده‌ای استفاده می‌شود.

۷-۲-۱ خط مشی‌های امنیتی و قواعد خط مشی‌های امنیتی

یک خط مشی امنیتی نشان‌دهنده‌ی الزامات امنیتی برای یک دامنه‌ی امنیتی است. برای مثال یک خط مشی امنیتی ممکن است الزاماتی را مشخص کند که به تمامی اعضای یک دامنه‌ی امنیتی که تحت یک شرایط خاص در حال فعالیت‌اند و یا این‌که به تمامی اطلاعات در یک دامنه‌ی امنیتی اعمال شود. پیاده‌سازی یک خط مشی امنیتی به این منجر خواهد شد که خدمات امنیتی نتیجه بخش و متناسب برای آن خط مشی امنیتی تعیین گردد و سازوکارهای امنیتی برای پیاده‌سازی خدمات امنیتی انتخاب شوند. انتخاب این‌که کدام سازوکارهای امنیتی انتخاب شوند به‌وسیله‌ی تهدیدات پیش‌بینی شده و ارزش منابعی که باید محافظت شوند، تحت تاثیر قرار می‌گیرد.

خط مشی‌های امنیتی به طور کلی همانند اصول کلی در زبان طبیعی هستند. این اصول الزامات امنیتی یک سازمان خاص یا اعضای یک دامنه‌ی امنیتی را منعکس می‌کنند. قبل از این‌که الزامات در سامانه‌های باز واقعی منعکس شوند، خط مشی امنیتی باید طوری پالایش[1] شود که یک مجموعه از قواعد خط مشی امنیتی را بتوان از آن استخراج کرد. تفسیری این الزامات به قواعد خط مشی امنیتی، فعالیتی مهندسی است. یک خط مشی امنیتی فعالیت عناصر را با توجه به آن خط مشی امنیتی یا با الزام به انجام عمل مورد نیاز خاص یا با جلوگیری از انجام فعالیتی خاص، محدود می‌کند. یک خط مشی امنیتی ممکن است به یک عنصر

1 - Refine

اجازه‌ی شرکت در فعالیت‌های خاصی را بدهد. این تفسیری کلی‌تر از تفسیری است که در توصیه‌نامه CCITT X.800 | ISO 7498-2 وجود داشته و تنها به OSI مربوط می‌شود. جنبه‌هایی از خط مشی امنیتی که مخصوص یک خدمت امنیتی خاص هستند، در چارچوب آن خدمت مورد بحث قرار می‌گیرند.

قواعد خط مشی امنیتی برای یک دامنه‌ی امنیتی دو گونه است، یکی آن‌هایی که برای فعالیت‌های درون یک دامنه‌ی امنیتی به‌کار می‌روند و دیگری آن‌هایی که برای فعالیت‌های بین دامنه‌های امنیتی به‌کار می‌روند. از قواعد خط مشی امنیتی از نوع دوم به عنوان قواعد برهم‌کنش امن تعبیر می‌شود. همچنین یک خط مشی امنیتی ممکن است تعیین کند که چه قواعدی به روابط با همه دامنه‌ها و چه قواعدی بر دامنه‌هایی خاص اعمال شوند.

قواعد خط مشی امنیتی باید با تغییر سامانه یا فعالیت‌ها و خط مشی امنیتی برای یک دامنه‌ی امنیتی معتبر باقی بماند.

یادآوری- این چارچوب به جنبه‌های زیر از خط مشی امنیتی توجه‌ای ندارد:

- طرفی[1] که یک خط مشي امنیتی را برقرار ساخته یا نگهداری می‌کند؛
- روال‌هایی که برای برقراری یا نگهداری یک خط مشي امنیتی به‌کار می‌روند؛
- محتوای یک خط مشي امنیتی؛
- روال‌هایی برای مقید کردن یک خط مشي امنیتی به یک دامنه‌ی امنیتی.

۷-۲-۲ مرجع دامنه‌ی امنیتی

یک هستار مرجع امنیتی هستاری است که مسئول پیاده‌سازی یک خط مشی امنیتی برای یک دامنه‌ی امنیتی است.

یک هستار مرجع دامنه‌ی امنیتی:

- ممکن است یک هستار مرکب باشد. اینچنین هستاری باید قابل تشخیص باشد؛
- ممکن است بسته به هر خط مشي امنیتی که هستار مرجع دامنه‌ی امنیتی ممکن است مورد توجه آن باشد، مسئولیت را برای پیاده‌سازی خط مشي امنیتی به یک یا چند هستار واگذار کند؛
- نسبت به عناصر موجود در دامنه‌ی امنیتی، مرجع باشد.

یادآوری- یک خط مشی امنیتی ممکن است بی‌ارزش[2] شود اگر هستار مرجع دامنه‌ی امنیتی تصمیم داشته باشد هیچ محدودیتی را اعمال نکند.

گفته می‌شود که دو هستار مرجع دامنه‌ی امنیتی با همدیگر می‌پیوندند اگر برای هماهنگ کردن خط مشی‌های امنیتی خود مقید شده باشند.

۷-۲-۳ روابط متقابل بین دامنه‌های امنیتی

مفهوم یک دامنه‌ی امنیتی به دو دلیل مهم است. که عبارتند از:

- می‌تواند برای توضیح چگونگی مدیریت امنیت به‌کار رود؛ و

1 - Party
2 - NULL

- می‌تواند به عنوان یک بلوك (بستك)[1] سازنده در مدل‌سازی فعالیت‌های امنیتی که عناصر تحت نظارت (مدیریت) هستارهای مرجع جداگانه را درگیر می‌کند، به‌کار رود.

دامنه‌های امنیتی به یک یا چند روش با همدیگر مرتبط می‌شوند. برخی از روابط ممکن دامنه‌ی امنیتی در اینجا مورد بررسی قرار می‌گیرند. روابط بین دامنه‌های امنیتی باید در خط مشی‌های امنیتی یک دامنه‌ی امنیتی همانگونه که هستارهای مرجع امنیتی بر روی آن توافق کرده‌اند، منعکس شده باشند. این روابط با استفاده از عناصر و فعالیت‌های دامنه‌های امنیتی بیان شده و در قواعد برهم‌کنش امن برای هر دامنه‌ی امنیتی مرتبط منعکس می‌شوند. برخی از روابط دامنه‌های امنیتی خاص در ادامه‌ی این قسمت توضیح داده می‌شوند. بسیاری دیگر از روابط دامنه‌های امنیتی امکان پذیر هستند.

الف- دو دامنه‌ی امنیتی جدا از یکدیگر خوانده می‌شوند اگر هیچ شئ داده‌ای و فعالیت مشترکی با یکدیگر نداشته باشند.

ب- دو دامنه‌ی امنیتی نسبت به یکدیگر مستقل خوانده می‌شوند اگر:

- هیچ شئ داده‌ای مشترکی نداشته باشند؛ و
- فعالیت‌های درون هر دامنه‌ی امنیتی تنها به‌وسیله‌ی خط مشي‌های امنیتی خود (و مجموعه‌ای از قواعد خط مشي‌های امنیتی معادل) محدود شده باشند؛ و
- هستارهای مرجع دامنه‌های امنیتی برای تنظیم کردن خط مشي‌های امنیتی خود محدود نشده باشند.
- دو یا چند دامنه‌ی امنیتی مستقل ممکن است برای به اشتراک‌گذاری اطلاعات بین یکدیگر، با همدیگر توافق کنند (به بند ۷-۲-٤ مراجعه کنید).

پ- دامنه‌ی امنیتی A یک *زیردامنه‌ی امنیتی* از دامنه‌ی امنیتی B خوانده می‌شود اگر و فقط اگر:

- مجموعه عناصر A زیرمجموعه‌ی مجموعه عناصر B بوده و یا با آن برابر باشد؛
- مجموعه‌ی فعالیت‌های درون A زیرمجموعه‌ی مجموعه‌ی فعالیت‌های درون B بوده و یا با آن برابر باشد؛
- اختیار قضاوت[2] نسبت به A از هستار مرجع B به هستار مرجع A تفویض شده باشد؛ و
- خط مشي امنیتی A با خط مشي امنیتی B تعارضی نداشته باشد. A ممکن است خط مشي امنیتی بیشتری را در صورت نیاز و در صورتی که خط مشي امنیتی B اجازه داده باشد، معرفی کند.

یادآوری ۱- یک زیرمجموعه ممکن است برابر *مجموعه بالادستی*[3] باشد. یک زیرمجموعه‌ی امنیتی ممکن است متشکل از تمامی مجموعه عناصر *دامنه‌ی امنیتی بالادستی*[4] برای برخی رده‌های فعالیت و یا متشکل از تمامی رده‌های فعالیت برای برخی زیرمجموعه‌های مجموعه عناصر دامنه‌ی امنیتی بالادستی باشد. بین این دو نوع، گونه‌های زیادی ممکن است وجود داشته باشد.

ت- دامنه‌ی امنیتی A یک *دامنه‌ی بالادستی* دامنه‌ی امنیتی B خوانده می‌شود اگر و فقط اگر B یک زیردامنه‌ی دامنه‌ی امنیتی A باشد.

---

1 - Block
2 - Justification
3 - Superset
4 - Super domain

یادآوری ۲- چارچوب‌های کاری امنیتی برای این‌که به‌وسیله‌ی هر پروتکل، مشخصه‌ها[1] یا پیاده‌سازی خاصی پشتیبانی شود، به مفاهیم جداشده، مستقل، زیردامنه و دامنه‌ی بالادستی نیازی ندارد.

۷-۲-۴ برقراری قواعد برهم‌کنش امن

برای این‌که بتوان بین دامنه‌های امنیتی تبادل اطلاعات داشت، باید مجموعه‌ای از قواعد خط مشی امنیتی مورد توافق برای این تبادل اطلاعات وجود داشته باشد. این قواعد خط مشی امنیت، قواعد برهم‌کنش امن نامیده می‌شوند. این قواعد بخشی از مجموعه قواعد خط مشی امنیتی هر دامنه‌ی امنیتی است. قواعد برهم‌کنش امن این امکان را فراهم می‌سازند که خدمات امنیتی و سازوکارهای عمومی در صورت امکان از طریق مذاکره انتخاب شده و اطلاعات امنیتی در هر دامنه‌ی امنیتی در صورت امکان از طریق نگاشت به یکدیگر مرتبط شوند. اطلاعات مدیریتی امنیتی مورد نیاز برای پشتیبانی از قواعد برهم‌کنشی امن ممکن است بین دامنه‌های امنیتی مبادله شوند. بسته به روابط بین دامنه‌های امنیتی، قواعد برهم‌کنشی امن به روش‌های مختلفی مشخص می‌شوند.

برای برهم‌کنش امن بین دامنه‌های مستقل، قواعد برهم‌کنشی امن باید از طریق مراجع امنیتی برای دامنه‌های امنیتی درگیر ارتباط، مورد پذیرش و توافق قرار گیرند.

برای برهم‌کنش بین دامنه‌های امنیتی، قواعد برهم‌کنشی امن را می‌توان به‌وسیله‌ی مراجع امنیتی دامنه بالادستی برقرار کرد. اگر خط مشی امنیتی دامنه‌ی امنیتی بالادستی اجازه داده باشد، زیردامنه‌های امنیتی قواعد برهم‌کنشی امن خاص خود را برقرار می‌کنند.

۷-۲-۵ انتقال بین دامنه‌ای اطلاعات امنیتی

قواعد برهم‌کنشی امن ممکن است خود اطلاعات امنیتی را مدیریت کنند و این اطلاعات امنیتی ممکن است نیاز داشته باشند که بین دامنه‌های امنیتی مبادله شوند. موارد زیر مد نظر هستند:

- معنا و بازنمایی اطلاعات امنیتی در هر دامنه‌ی امنیتی می‌توانند یکسان باشند. این بدان معنی است که برگردان آن‌ها ضروری نیست.
- معنای اطلاعات امنیتی در هر دامنه‌ی امنیتی یکسان اما نمایش آن‌ها با یکدیگر متفاوت است. این بدان معنی است که روشی که به‌وسیله‌ی آن اطلاعات امنیتی توصیف می‌شوند متفاوت بوده و بنابراین برگردان نحو مورد نیاز است.
- معنا و بازنمایی اطلاعات امنیتی در هر دامنه‌ی امنیتی متفاوت است. این بدان معنی است که قواعد برهم‌کنشی امن باید چگونگی برگردان اطلاعات از یک دامنه امنیتی به یک دامنه‌ی امنیتی دیگر را مشخص کند. برگرداندن نحو ممکن است ضروری باشد.

۷-۳ ملاحظات خط مشی امنیتی برای خدمات امنیتی خاص

سازوکارهای کنترل دسترسی ممکن است در برخی پیاده‌سازی‌های یک خدمت یکپارچگی یا یک خدمت محرمانگی مورد استفاده قرار گیرند. در چنین مواردی قواعد خط مشی امنیتی مرتبط با پیاده‌سازی یک خدمت یکپارچگی یا یک خدمت محرمانگی باید چگونگی مورد استفاده قرار گرفتن سازوکارهای کنترل

1 - Specification

دسترسی را توصیف کنند. سازوکارهای کنترل دسترسی با استفاده از آغازگران[1] و اهداف[2] (در توصیه‌نامه ITU-T X.812 |ISO/IEC 10181-3) توضیح داده می‌شوند. قواعد خط مشی امنیتی چگونگی ارتباط هستارها، واحدهای داده و اطلاعات در خط مشی‌های محرمانگی و یکپارچگی با آغازگران و اهداف در سازوکارهای کنترل دسترسی را تعریف می‌کنند.

خط مشی‌های محرمانگی به این صورت که کدام هستارها باید واحدهای اطلاعاتی را بررسی کنند، بیان می‌شوند. یک عمل انجام شده به‌وسیله‌ی یک آغازگر بر روی یک هدف به دو روش می‌تواند اطلاعات را در دسترس یک هستار قرار دهد. اول اینکه، نتیجه‌ی یک عمل ممکن است اطلاعاتی در مورد هدف را در اختیار آغازگر قرار دهد. دوم اینکه، درخواست عمل ممکن است اطلاعاتی در مورد آغازگر را در اختیار هدف قرار دهد. هنگامی که سازوکارهای کنترل دسترسی مورد استفاده قرار می‌گیرند تا یک خدمت محرمانگی را فراهم کنند، هستارهایی که برای کسب اطلاعات در تلاش هستند به عنوان آغازگران و فقره‌های[3] اطلاعاتی به عنوان اهداف در نظر گرفته می‌شوند.

خط مشی‌های یکپارچگی به این صورت که کدام هستارها ممکن است واحدهای داده را تغییر دهند، بیان می‌شوند. یک عمل انجام شده به‌وسیله‌ی یک آغازگر بر روی یک هدف به دو روش می‌تواند داده‌ها را تغییر دهد. اول این‌که عمل ممکن است به‌طور مستقیم داده‌های موجود در هدف را تغییر دهد. دوم این‌که نتیجه‌ی عمل ممکن است منجر به تغییر اطلاعات موجود در آغازگر شود. هنگامی که سازوکارهای کنترل دسترسی برای فراهم کردن یک خدمت یکپارچگی مورد استفاده قرار می‌گیرند، هستارهایی که برای تغییر داده‌ها در تلاش هستند به عنوان آغازگران و واحدهای داده به عنوان اهداف در نظر گرفته می‌شوند.

۴-۷ هستارهای قابل اعتماد

یک هستار برای برخی رده‌ها در زمینه‌ی یک خط مشی امنیتی قابل اعتماد نامیده می‌شود اگر بتواند با انجام دادن اعمالی که نباید انجام دهد و یا عدم انجام اعمالی که باید انجام دهد، از خط مشی امنیتی تخطی کند. خط مشی امنیتی تعیین می‌کند که چه هستارهایی قابل اعتماد هستند. علاوه بر این مجموعه‌ی فعالیت‌ها برای هر هستار قابل اعتماد را نیز مشخص می‌کند. یک هستار که برای انجام یک مجموعه از عملیات قابل اعتماد شناخته می‌شود ضروری نیست که برای تمامی فعالیت‌های درون یک دامنه‌ی امنیتی قابل اعتماد باشد.

بیان این موضوع در یک خط مشی امنیتی که یک هستار باید به روشی مشخص رفتار کند به‌طور الزامی تضمین نمی‌کند که هستار مورد نظر با آن روش مشخص رفتار می‌کند. بنابراین، یک خط مشی امنیتی ممکن است نیازمند آن باشد که ابزارهایی برای تشخیص تخطی از خط مشی امنیتی به‌وسیله‌ی بدرفتاری یک هستار قابل اعتماد داشته باشد. یک هستار قابل اعتماد که بدون این‌که تشخیص داده شود می‌تواند رفتار نامناسبی از خود نشان دهد به عنوان یک *هستار قابل اعتماد بدون شرط* شناخته می‌شود. یک هستار قابل

1 - Initiators
2 - Targets
3 - Items

اعتماد که می‌تواند از خط مشی امنیتی تخطی کند اما نمی‌تواند این کار را بدون این‌که تشخیص داده شود انجام دهد به عنوان یک *هستار قابل اعتماد مشروط* شناخته می‌شود.

یک هستار قابل اعتماد ممکن است برای زیرمجموعه‌ای از فعالیت‌هایش به صورت بدون شرط قابل اعتماد باشد در حالی که برای یک زیرمجموعه‌ی متفاوت از فعالیت‌هایش به صورت مشروط قابل اعتماد باشد. چنین هستاری در مواردی می‌تواند بدون این‌که شناخته شود از خط مشی امنیتی تخطی کرده اما نمی‌تواند در مواردی دیگر بدون این‌که تشخیص داده شود از خط مشی امنیتی تخطی کند.

یک خط مشی امنیتی مربوط به یک دامنه‌ی امنیتی ممکن است مشخص کند که یک عنصر که در دامنه‌ی امنیتی وجود ندارد برای برخی از عملیات درون دامنه‌ی امنیتی قابل اعتماد باشد. قواعد برهم‌کنشی امن (آن گونه که در بند ۷-۲-۴ توضیح داده شد) ممکن است چگونگی برهم‌کنش هستارهای درون دامنه‌ی امنیتی با هستارهای قابل اعتماد خارج از دامنه‌ی امنیتی را مشخص کنند.

۷-۵ اعتماد

گفته می‌شود که هستار X به هستار Y برای انجام مجموعه‌ای از فعالیت‌ها *اعتماد دارد* اگر و تنها اگر هستار X به هستار Y رفتارکننده به روشی خاص با در نظر گرفتن فعالیت‌ها، اتکا داشته باشد.

اعتماد در صورت لزوم دوطرفه نیست. یک هستار که قابل اعتماد نیست ممکن است از خدمات فراهم شده به‌وسیله‌ی یک هستار قابل اعتماد استفاده کند. به عنوان مثالی از موقعیتی که در آن اعتماد دوطرفه است می‌توان به زمانی اشاره کرد که هستارهای قابل اعتماد برای انجام دادن یک عمل با همدیگر همکاری کرده و هر یک از آن دو به این‌که دیگری در اعمال خط مشی امنیتی به آن کمک کند، تکیه داشته باشد.

اعتماد در صورت لزوم تراگذری (متعدی)[1] نیست. یک خط مشی امنیتی ممکن است تراگذر بودن اعتماد را در مواردی خاص تعریف کند. اگر هستار A به خدمات فراهم شده به‌وسیله‌ی هستار قابل اعتماد B، و هستار قابل اعتماد B به خدمات فراهم شده به‌وسیله‌ی هستار قابل اعتماد C تکیه داشته باشد، آنگاه A ممکن است به طور غیرمستقیم به این‌که C به روشی مشخص رفتار کند، تکیه داشته باشد. در نمونه‌هایی که این مورد اتفاق می‌افتد، اعتماد تراگذر است. اما در بقیه‌ی موارد B باید ثابت کند که رفتار نامناسب C نمی‌تواند فعالیت‌های A را تحت تاثیر قرار دهد. در این موارد اعتماد تراگذر نیست.

۷-۶ طرف‌های سوم قابل اعتماد

یک طرف سوم قابل اعتماد یک مرجع امنیتی یا عامل آن بوده که با توجه به برخی فعالیت‌های امنیتی در زمینه‌ی یک خط مشی امنیتی قابل اعتماد است.

نمونه‌هایی از طرف‌های سوم قابل اعتماد عبارتند از:

- یک طرف سوم قابل اعتماد در احراز هویت؛
- یک خدمت ثبت یا برچسب‌دهی زمانی در انکارناپذیری؛
- یک مرکز توزیع کلید در مدیریت کلید.

1 - Transitive

۸ اطلاعات امنیتی عمومی

برخی از اطلاعات امنیتی در بیش از یک چارچوب کاری امنیتی مورد نیاز است. این بند این انواع اطلاعات امنیتی را توصیف می‌کند.

سازوکارهای امنیتی توضیح داده شده در چارچوب‌های کاری امنیتی به طور معمول شامل تبادل اطلاعات امنیتی بین هستارهایی که برای یک برهم‌کنش نیازمند خدمات امنیتی بوده یا شامل تبادل اطلاعات بین یک مرجع امنیتی و هستارهای برهم‌کنشی[1] است. چهار شکل عمومی از اطلاعات امنیتی که به‌وسیله‌ی سازوکارها مورد استفاده قرار می‌گیرند و در این چارچوب توضیح داده می‌شوند عبارتند از:

- برچسب‌های امنیتی استفاده شده برای تشخیص خط مشي امنیتی قابل اعمال به یک عنصر، یک کانال ارتباطی یا یک قلم داده؛
- مقادیر وارسی رمزنگاشتي مورد استفاده برای تشخیص تغییرات یک واحد داده؛
- گواهی‌های امنیتی مورد استفاده برای محافظت از اطلاعات امنیتی به‌دست آمده از یک مرجع امنیتی یا طرف سوم قابل اعتماد برای استفاده به‌وسیله‌ی یک یا چند طرف که با هم برهم‌کنش دارند؛
- نشانه‌های امنیتی مورد استفاده برای محافظت از اطلاعات امنیتی مبادله شده بین طرف‌های برهم‌کنشی.

یادآوری- اطلاعات امنیتی می‌توانند به‌وسیله‌ی چندین سازوکار امنیتی مختلف محافظت شوند. برخی سازوکارهای امنیتی مبتنی بر استفاده از رمزنگاری هستند. در حالی که سایر سازوکارها از ابزارهای فیزیکی استفاده می‌کنند.

۸-۱ برچسب‌های امنیتی

یک برچسب امنیتی مجموعه‌ای از خصوصیت‌های امنیتی است که به یک عنصر، کانال ارتباطی یا واحد داده مقید می‌شود. یک برچسب امنیتی همچنین به صورت صریح یا ضمنی، مرجع امنیتی رابط، و خط مشی امنیتی قابل اعمال برای استفاده از برچسب‌ها را تعیین می‌کند. یک برچسب امنیتی برای پشتیبانی از ترکیبی از خدمات امنیتی مورد استفاده قرار می‌گیرد.

نمونه‌هایی از موارد استفاده از برچسب‌های امنیتی عبارتند از:

- پشتیبانی از یک شمای کنترل دسترسی مبتنی بر برچسب، شامل کاربرد کنترل دسترسی برای فراهم ساختن یکپارچگي و/یا محرمانگی؛
- تعیین درجه اطمینان قابل جایگذاری در داده و الزامات به‌کار بردن آن؛
- تعیین حساسیت داده و الزامات به‌کاربردن آن؛
- تعیین محافظت، دسترسی و سایر الزامات به کار بردن آن.

۸-۲ مقادیر وارسی رمزنگاشتی

یک مقدار وارسی رمزنگاشتی اطلاعاتی است که با انجام تبدیلات رمزنگاری یک واحد داده به‌دست می‌آید. مهرها، امضاهای رقمی و اثرانگشت‌های رقمی سه نمونه از مقادیر وارسی رمزنگاشتی هستند.

1 - Interacting

یک مهر شکلی از یک مقدار وارسی رمزنگاشتی است که به‌وسیله‌ی الگوریتم رمزنگاشتی متقارن و یک کلید سرّی به اشتراک گذاشته شده به‌وسیله‌ی هستارهای ارتباطی محاسبه می‌شود. مهرها برای تشخیص تغییر داده‌ها در طول انتقال مورد استفاده قرار می‌گیرند.

یک امضای دیجیتالی یک مقدار وارسی رمزنگاشتی است که از جعل اسناد به‌وسیله‌ی دریافت کننده جلوگیری کرده و به‌وسیله‌ی یک کلید خصوصی و یک الگوریتم رمزنگاشتی نامتقارن محاسبه می‌شود. بررسی یکپارچگی امضای دیجیتالی نیازمند استفاده از همان الگوریتم رمزنگاشتی و کلید عمومی معادل با کلید خصوصی است.

یادآوری ۱- اگرچه ابزارهای دیگری برای جلوگیری از جعل مقادیر وارسی رمزنگاشتی به‌وسیله‌ی دریافت کننده وجود دارد (به عنوان نمونه استفاده از پودمان‌های رمزنگاری مقاوم در برابر دست‌کاری[1])، چارچوب‌های کاری امنیتی از عبارت امضای دیجیتالی به معنی یک مقدار وارسی رمزنگاشتی استفاده کرده که با استفاده از یک الگوریتم رمزنگاشتی نامتقارن به‌دست آمده است.

یادآوری ۲- با برخی الگوریتم‌های رمزنگاشتی نامتقارن، محاسبه‌ی یک امضای دیجیتالی نیازمند استفاده از بیش از یک کلید خصوصی است. هنگامی که از چنین الگوریتم‌هایی استفاده می‌شود، داشتن هر یک از کلیدهای خصوصی به برخی از هستارها محدود می‌شود. این کار تضمین می‌کند هستارها باید برای ایجاد یک امضای دیجیتالی با همدیگر همکاری داشته باشند.

یک اثرانگشت رقمی خصوصیتی از یک واحد داده است که به اندازه‌ی کافی برای آن واحد داده نامانوس[2] است، به طوری که از نظر محاسباتی یافتن واحد داده‌ای دیگری با آن اثرانگشت رقمی غیرممکن است.

برخی از اشکال مقدار وارسی رمزنگاشتی (به عنوان مثال نتیجه‌ی اعمال یک تابع یک سویه بر داده) را می‌توان برای ایجاد یک اثرانگشت رقمی مورد استفاده قرار داد. اثرانگشت‌های رقمی می‌توانند با روشی غیر از الگوریتم‌های رمزنگاشتی ایجاد شوند. برای مثال، یک رونوشت[3] از واحد داده یک اثرانگشت رقمی است.

یادآوری ۳- توابع یک سویه با اثرانگشت‌های رقمی هم‌ارز نیستند و برخی از اثرانگشت‌ها به‌وسیله‌ی توابع یک سویه ایجاد نمی‌شوند.

یادآوری ۴- محاسبه‌ی یک امضای دیجیتالی با استفاده از یک الگوریتم نامتقارن می‌تواند مدت زمان زیادی طول بکشد چرا که الگوریتم‌های نامتقارن به طور کلی از نظر محاسباتی پیچیدگی بالایی دارند. یک امضای دیجیتالی ممکن است از روی یک اثرانگشت رقمی یک داده به جای خود داده محاسبه شود. این امر منجر به کارایی بهتری می‌شود. چرا که این کار می‌تواند برای محاسبه‌ی یک امضای دیجیتالی از روی یک اثرانگشت کوتاه رقمی سریعتر از محاسبه‌ی آن از روی یک پیام طولانی انجام شود.

یک مقدار وارسی رمزنگاشتی، ضروری نیست در برابر بازپخش یک واحد داده محافظت ایجاد کند. محافظت در برابر بازپخش را می‌توان به‌وسیله‌ی قرار دادن برخی اطلاعات که برای محافظت در برابر بازپخش مورد

1 - Tamper
2 - Peculiar
3 - Copy

استفاده قرار می‌گیرند مانند شماره ترتیب[1] یا برچسب زمانی درون داده یا با استفاده از زنجیره‌ی رمزنگاشتی انجام داد. برای محافظت در برابر بازپخش، این اطلاعات باید به‌وسیله‌ی دریافت‌کننده‌ی واحدهای داده‌ای محافظت شده، بررسی شوند.

۸-۳ گواهی‌های امنیت

۸-۳-۱ مقدمه‌ای بر گواهی‌های امنیتی

یک گواهی امنیتی مجموعه‌ای از داده‌های امنیتی منتشر شده به‌وسیله‌ی یک هستار مرجع امنیتی یا یک طرف سوم قابل اعتماد، به علاوه‌ی اطلاعات امنیتی که برای فراهم ساختن خدمات یکپارچگی و احراز هویت مبدأ داده مورد استفاده داده‌ها، است. یک گواهی امنیتی شامل دوره‌های زمانی است که در آن دوره‌ها داده‌ها دارای اعتبارند.

گواهی‌های امنیتی برای حمل اطلاعات امنیتی از یک هستار مرجع امنیتی (یا یک طرف سوم قابل اعتماد) به هستارهایی که برای اجرای کارکرد امنیتی به آن اطلاعات نیازمند هستند، به‌کار می‌روند. یک گواهی امنیتی ممکن است شامل اطلاعات امنیتی برای بیش از یک خدمت امنیتی باشد.

همانطور که در چارچوب‌های کاری دیگر توضیح داده شد، یک گواهی امنیتی ممکن است شامل اطلاعاتی امنیتی باشد که برای موارد زیر به‌کار می‌روند:

- اهداف کنترل دسترسی؛
- اهداف احراز هویت؛
- اهداف یکپارچگی؛
- اهداف محرمانگی؛
- اهداف انکارناپذیری؛
- اهداف ممیزی؛
- اهداف مدیریت کلید.

۸-۳-۲ درستی‌سنجی و زنجیره‌سازی گواهی‌های امنیتی

درستی‌سنجی یک گواهی امنیتی شامل اعتبارسنجی[2] یکپارچگی آن، اعتبارسنجی هویتی که به‌وسیله‌ی مرجع آن ادعا می‌شود و بررسی مجاز بودن مرجع برای صدور گواهی امنیتی است. این عملیات ممکن است به اطلاعات امنیتی بیشتری نیاز داشته باشند.

اگر درستی‌سنج گواهی‌های امنیتی اطلاعات امنیتی مورد نیاز برای تعیین یکپارچگی گواهی امنیتی را نداشته باشد، یک گواهی امنیتی از یک هستار مرجع امنیتی دیگر ممکن است برای تامین اطلاعات امنیتی ضروری مورد استفاده قرار گیرد. این فرآیند برای ایجاد یک زنجیره از گواهی‌های امنیتی می‌تواند تکرار شود. این‌ها اطلاعات امنیتی را حمل می‌کنند که یک مسیر مطمئن از هستار مرجع امنیتی به آن هستار را به فراهم می‌آورند.

---

1 - Sequence number
2 - Validation

یک زنجیره از گواهی‌های امنیتی تنها زمانی می‌تواند مورد استفاده قرار گیرد که محدودیت‌های اعمال شده به‌وسیله‌ی خط مشی‌های امنیتی مرتبط را برآورده سازد. وجود یک زنجیره کافی نیست. تنها زمانی می‌توان از یک زنجیره استفاده کرد که اجازه‌ی استفاده از آن به‌وسیله‌ی روابط مورد اعتماد بین درستی‌سنج یک زنجیره و هستارهای مرجع امنیتی ایجاد کننده‌ی زنجیره‌ی گواهی‌های امنیتی و همچنین به‌وسیله‌ی روابط قابل اعتماد بین آن هستارهای مرجع امنیتی صادر شده باشد. این روابط به‌وسیله‌ی خط مشی امنیتی مربوط به درستی‌سنجی زنجیره‌ی گواهی و خط مشی‌های امنیتی مربوط به هستارهای مرجع امنیتی تعریف و مشخص می‌شوند. به خصوص برخی از هستارهای مرجع امنیتی برای صادر کردن گواهی امنیتی برای برخی دیگر از هستارهای مرجع امنیتی مورد اعتماد هستند. در حالی که برخی از سایر هستارهای مرجع امنیتی تنها برای صدور گواهی‌های امنیتی برای هستارهایی که خود مدیریت می‌کنند، مورد اعتماد هستند.

۸-۳-۳ لغو گواهی‌های امنیتی

اطلاعات امنیتی موجود در یک گواهی امنیتی ممکن است دیگر معتبر نباشد. برای مثال اگر یک کلید خصوصی به خطر بیافتد، آنگاه کلید عمومی معادل دیگر نباید مورد استفاده قرار گیرد و از این رو گواهی‌های امنیتی که شامل این کلید هستند باید لغو شوند.

سازوکارهایی که می‌توانند برای لغو گواهی امنیتی مورد استفاده باشند شامل گواهی‌های لغو و گواهی‌های فهرست لغو هستند. یک *گواهی لغو* یک گواهی امنیتی است که مشخص می‌کند یک گواهی خاص لغو شده است. یک *گواهی فهرست لغو* یک گواهی امنیتی است که فهرستی از گواهی‌های امنیتی لغو شده را مشخص می‌کند.

۸-۳-۴ استفاده‌ی مجدد از گواهی‌های امنیتی

برخی گواهی‌های امنیتی به منظور پشتیبانی از بیش از یک نمونه ارتباط به‌کار می‌روند. در حالی که سایر گواهی‌ها تنها یکبار مورد استفاده قرار می‌گیرند. نمونه‌ای از یک گواهی امنیتی که بیش از یکبار مورد استفاده قرار می‌گیرد، گواهی احراز هویت تعریف شده در توصیه‌نامه ITU-T X.509 | ISO/IEC 9594-8 است. نمونه‌ای از یک گواهی امنیتی که تنها یکبار مورد استفاده قرا می‌گیرد، گواهی کنترل دسترسی است که مجاز بودن دسترسی را مشخص می‌کند. گواهی امنیتی که تنها یکبار مورد استفاده قرار می‌گیرد ممکن است شامل اطلاعاتی باشد که از استفاده‌ی مجدد آن جلوگیری کند.

۸-۳-۵ ساختار گواهی امنیتی

شکل کلی یک گواهی امنیتی سه قسمت اصلی دارد که عبارتند از:

- اطلاعات مورد نیاز در تمامی گواهی‌های امنیتی؛
- اطلاعات امنیتی مربوط به یک یا چند خدمت امنیتی؛
- اطلاعاتی برای کنترل یا محدود کردن استفاده از اطلاعات امنیتی.

اطلاعات امنیتی مورد نیاز در تمامی گواهی‌های امنیتی به دو دسته‌ی کلی تقسیم می‌شود که عبارتند از:

الف- اطلاعاتی که هم یکپارچگی و هم احراز هویت مبدأ داده‌ها (مانند یک مقدار وارسی رمزنگاشتی و تعیین کردن اطلاعات مورد استفاده برای درستی‌سنجی آن) را فراهم می‌کند. از آنجا که خدمت احراز هویت مبدأ داده‌ها فراهم می‌شود، احراز هویت منبع ادعا شده‌ی گواهی امنیتی نیز باید فراهم شود.

ب- اطلاعاتی که از روی آن می‌توان دوره‌ای از اعتبار را تشخیص داد (مانند دوره‌ی اعتبار صریح) و یا دریافت کرد (مانند دوره‌ی اعتبار ضمنی). این اطلاعات باعث جلوگیری از استفاده‌ی مجدد از گواهی امنیتی می‌شود هرچند که گواهی امنیتی ممکن است بارها مجددا در دوره‌ی اعتبار مورد استفاده قرار گیرد.

اطلاعاتی که برای کنترل یا محدود کردن استفاده از اطلاعات امنیتی به‌کار می‌روند به سه دسته تقسیم می‌شوند که عبارتند از:

الف- اطلاعاتی که برای محافظت از استفاده‌ی غیرمجاز گواهی امنیتی به‌کار می‌روند.

مثال‌ها عبارتند از:

- اطلاعاتی (مانند یک شناسه تمیز دهنده) که هستار یا هستارهایی را مشخص می‌کند که اطلاعات امنیتي آن‌ها در گواهی امنیتی موجود است.
- اطلاعاتی که هستارهایی را مشخص می‌کند که مجاز به استفاده از اطلاعات موجود در گواهی امنیتی هستند؛
- اطلاعاتی که تعداد دفعاتی را که گواهی مورد استفاده قرار گرفته است کنترل می‌کند؛
- اطلاعاتی که خط مشي امنیتی را که تحت آن گواهی امنیتی باید مورد استفاده قرار بگیرد، مشخص می‌کند؛
- روش‌های محافظت و پارامترهای مرتبط برای محافظت از گواهی امنیتی در برابر سرقت[1] (به پیوست الف مراجعه کنید)؛
- اطلاعات مورد استفاده برای محافظت در برابر بازپخش (مانند یک عدد یکتا یا یک چالش).

ب- اطلاعاتی که برای کمک به یک ممیزی امنیتی می‌تواند مورد استفاده قرار گیرند.

مثال‌ها عبارتند از:

- یک شناسه مرجع برای گواهی امنیتی (مانند یک شماره پي‌درپي[2]) که برای گواهی امنیتی که برای تمامی گواهی‌های امنیتی صادر شده به‌وسیله‌ی یک مرجع امنیتی یا عامل آن، یکتا است؛
- هویت (برای اهداف ممیزی) یک هستار که گواهی امنیتی در ابتدا برای آن صادر شده است.

پ- اطلاعاتی که برای کمک به یک بازیابی امنیتی می‌تواند مورد استفاده باشد.

مثال‌ها عبارتند از:

- یک شناسه مرجع برای گواهی امنیتی که برای لغو یک گواهی امنیتی خاص می‌تواند مورد استفاده باشد؛
- یک شناسه گروه برای گواهی امنیتی که برای لغو یک گروه خاص از گواهی‌های امنیتی می‌تواند مورد استفاده باشد.

1 - Theft
2 - Serial number

۸-۴ نشانه‌های امنیتی

یک نشانه‌ی امنیتی مجموعه‌ای از داده‌های محافظت شده به‌وسیله‌ی یک یا چند خدمت امنیتی، به اضافه‌ی اطلاعات امنیتی است که برای فراهم ساختن آن خدمات امنیتی به‌کار می‌رود و بین هستارهای ارتباطی مبادله می‌شوند. نشانه‌های امنیتی می‌توانند بر اساس سازنده‌ی آن‌ها و نوع خدمات امنیتی مورد استفاده برای محافظت از محتوای آن‌ها دسته‌بندی شوند.

یک نشانه‌ی امنیتی که به‌وسیله‌ی یک هستار مرجع امنیتی صادر شده و به‌وسیله‌ی خدمات احراز هویت مبدأ داده‌ها و یکپارچگی محافظت می‌شود به عنوان یک گواهی امنیتی شناخته می‌شود. (به بند ۸-۳ مراجعه کنید).

بسیاری از سازوکارهای امنیتی نیازمند مبادله‌ی محافظت شده برای یکپارچه‌سازی اطلاعات امنیتی بین دو هستار ارتباطی بوده که هیچ یک از آن دو هستار، مرجع امنیتی نیستند. نشانه‌های امنیتی مورد استفاده برای دسترسی به این مبادلات یکپارچه، گواهی‌های امنیتی نیستند. چرا که هستارهای ایجاد کننده‌ی آن‌ها، هستارهای مرجع امنیتی نیستند. اینچنین نشانه‌های امنیتی به عنوان *نشانه‌های امنیتی یکپارچه* شناخته می‌شوند.

تمامی نشانه‌های امنیتی یکپارچه شامل اطلاعات زیر هستند:

- اطلاعاتی که هم احراز هویت مبدأ داده‌ها و هم یکپارچگی داده‌ها را تامین می‌کند (مانند یک مقدار وارسی رمزنگاشتی و یا اطلاعاتی که برای درستی‌سنجی آن به‌کار می‌رود).

یک نشانه‌ی امنیتی یکپارچه ممکن است شامل یک یا چند مورد از اطلاعات اضافی زیر نیز باشد:

- اطلاعاتی که از آن اعتبار یک دوره‌ی زمانی قابل تشخیص است؛
- اطلاعاتی که برای محافظت در برابر بازپخش استفاده می‌شوند (برای مثال یک شماره‌ی یکتا).

۹ تسهیلات امنیتی کلی

بسیاری از تسهیلات در بیش از یک چارچوب کاری امنیتی مورد نیاز هستند. این بند، این تسهیلات را برای استفاده در سایر چارچوب‌های کاری امنیتی معرفی می‌کند.

۹-۱ تسهیلات مرتبط با مدیریت

این زیربند انواع تسهیلات کلی مدیریتی را مشخص می‌کند. ممکن است زیربندهایی از این تسهیلات مدیریتی که خاص یک سازوکار مشخص است، وجود داشته باشند.

۹-۱-۱ نصب اطلاعات امنیتی[1]

این امکان[2]، یک مجموعه‌ی اولیه از اطلاعات امنیتی مقید به یک عنصر را فراهم می‌سازد.

1 - Install SI
2 - Facility

۹-۱-۲ حذف اطلاعات امنیتی[1]

این امکان باعث می‌شود یک هستار از دامنه‌ی امنیتی حذف شود که این کار را با لغو اطلاعات امنیتی که مشخص می‌کند آن هستار عضوی از دامنه‌ی امنیتی است، انجام می‌دهد.

۹-۱-۳ تغییر اطلاعات امنیتی[2]

این تسهیلات برای تغییر اطلاعات امنیتی مرتبط با یک عنصر مورد استفاده قرار می‌گیرد.

۹-۱-۴ اعتبارسنجی اطلاعات امنیتی[3]

این تسهیلات یک مجموعه از اطلاعات امنیتی را به یک عنصر مقید می‌کند. این امکان به‌وسیله‌ی یک هستار مرجع امنیتی یا عامل آن فراخوانی می‌شود.

۹-۱-۵ بی‌اعتبارکردن اطلاعات امنیتی[4]

این تسهیلات هر استفاده‌ای از اطلاعات امنیتی مرتبط با یک عنصر را غیرفعال می‌کند. این امکان به‌وسیله‌ی یک هستار مرجع امنیتی یا عامل آن فراخوانی می‌شود. اطلاعات امنیتی که به‌وسیله‌ی این امکان غیرفعال شده‌اند ممکن است برای اهداف ممیزی یا اطمینان از غیرفعال ماندن اطلاعات امنیتی، کماکان درون سامانه ذخیره باقی بمانند.

۹-۱-۶ غیرفعال/فعال‌سازی مجدد خدمت امنیتی[5]

این تسهیلات جنبه‌های مشخصی از یک خدمت امنیتی را غیرفعال یا دوباره فعال‌سازی می‌کند.

۹-۱-۷ عضویت[6]

این تسهیلات باعث می‌شود تا یک هستار مرجع امنیتی برخی اطلاعات امنیتی مرتبط با یک هستار را ثبت کند. این تسهیلات ممکن است به‌وسیله‌ی یک هستار که هستار مرجع امنیتی نیست، مورد استفاده قرار گیرد. برای مثال یک هستار که مایل به پیوستن به یک دامنه‌ی امنیتی است می‌تواند با استفاده از این امکان از تمایل خود به پیوستن به دامنه‌ی امنیتی برای مطلع ساختن یک هستار مرجع امنیتی استفاده کند.

۹-۱-۸ لغو عضویت[7]

این تسهیلات باعث می‌شود که یک عنصر از یک دامنه‌ی امنیتی حذف شده و اطلاعات امنیتی مرتبط با آن نیز لغو شود. این امکان به‌وسیله‌ی یک هستار مرجع امنیتی یا عامل آن مورد استفاده قرار می‌گیرد. یک خط مشی امنیتی ممکن است به برخی از انواع اطلاعات امنیتی که هرگز از بین نمی‌روند نیاز داشته باشد.

---

1 - De-install SI
2 - Change SI
3 - Validate SI
4 - Invalidate SI
5 - Disable/Re-enable security service
6 - Enroll
7 - Un-enroll

۹-۱-۹ توزیع اطلاعات امنیتی[1]

این تسهیلات برای در دسترس قرار دادن قسمت‌هایی از اطلاعات امنیتی برای سایر هستارها به‌وسیله یک هستار مرجع امنیتی یا عامل آن مورد استفاده قرار می‌گیرد.

۹-۱-۱۰ اطلاعات امنیتی فهرست[2]

این تسهیلات، اطلاعات امنیتی مقید به یک عنصر را فهرست می‌کند.

۹-۲ تسهیلات مربوط به عملیات[3]

۹-۲-۱ تشخیص هستارهای مرجع مورد اعتماد

این تسهیلات، آن دسته از هستارهای مرجع امنیتی را که در زمینه‌ی یک خط مشی امنیتی برای عناصر یا فعالیت‌های خاصی مورد اعتماد هستند مشخص می‌کند. (به عنوان مثال برای فراهم کردن کلیدهای رمزگذاری، گواهی‌های امنیتی کنترل دسترسی و یا گواهی‌های امنیتی احراز هویت).

۹-۲-۲ شناسایی قواعد برهم‌کنش امن

این تسهیلات، قواعد برهم‌کنش امن را برای استفاده شناسایی می‌کند. این امر ممکن است از طریق اطلاعات از پیش جمع‌آوری شده و یا از طریق مذاکره بین عناصر دامنه‌های مرتبط با یکدیگر همانطور که در ۷-۲-۴ شرح داده شد، انجام شود.

یادآوری- قواعد برهم‌کنشی امن از طریق توافق بین دامنه‌های امنیتی برقرار می‌شوند نه با استفاده از این امکانات. این امکان تعیین می‌کند که کدام یک از قواعد برهم‌کنشی امن از پیش برقرار شده، برای یک فعالیت خاص قابل اعمال است.

۹-۲-۳ به‌دست آوردن اطلاعات امنیتی

این تسهیلات، اطلاعات امنیتی را قبل از انجام دادن فعالیت می‌پذیرد.

نمونه‌هایی از زیررده‌های این امکان عبارتند از:

- کنترل دسترسی: گرفتن آغازگر ACI، گرفتن هدف ACI؛
- احراز هویت: پذیرفتن.

۹-۲-۴ ایجاد اطلاعات امنیتی

این تسهیلات، اطلاعات امنیتی برای یک فعالیت مقید به امنیت را ایجاد می‌کند. این اطلاعات امنیتی ممکن است به داده‌ها مقید باشند.

نمونه‌هایی از زیررده‌های این امکان عبارتند از:

- کنترل دسترسی: وابسته‌سازي عمل ACI؛
- احراز هویت: ایجاد؛
- انکارناپذیري: ایجاد مدرک.

---

1 - Distribute SI
2 - List SI
3 - Operational related facilities

۹-۲-۵ درستی‌سنجی اطلاعات امنیتی

این تسهیلات امنیتی اعتبار اطلاعات امنیتی ایجاد شده با استفاده از امکان ساخت اطلاعات امنیتی را درستی‌سنجی می‌کند. امکان درستی‌سنجی SI ممکن است خود، اطلاعات امنیتی را برای این‌که در اختیار استفاده‌ای دیگر از این امکان قرار گیرند ایجاد کند.

نمونه‌هایی از زیررده‌های این امکان عبارتند از:

- کنترل دسترسی: درستی‌سنجي عمل ACI؛
- احراز هویت: درستی‌سنجي؛
- انکارناپذیري: اعتبارسنجی مدارک.

مثالی از موقعیتی که در آن خروجی امکان درستی‌سنجی اطلاعات امنیتی برای درستی‌سنجی بیشتر به عقب برگشت می‌شود، پروتکل دو طرفه برای احراز هویت دوطرفه است. فرض کنید هستارهای A و B مایلند یکدیگر را احراز هویت کنند و هستار A تبادل پروتکل را آغاز می‌کند. هستار A امکان ساخت اطلاعات امنیتی را برای ایجاد اطلاعات امنیتی احراز هویت که شامل مدرکی دال بر هویت A و چالشی است که هستار B باید به آن پاسخ‌گو باشد، اجرا می‌کند. هستار B امکان درستی‌سنجی اطلاعات امنیتی را برای بررسی این‌که آیا چالش از طرف A فرستاده شده است، فراخوانی کرده و همچنین اطلاعات احراز هویت جدیدی محتوی مدرکی در مورد هویت B و پاسخی که به چالش A می‌دهد، می‌سازد. پس از آن هستار A وسیله‌ی سهولت درستی‌سنجی اطلاعات امنیتی را برای بررسی این‌که جواب از طرف B صادر شده و با چالش اصلی مطابقت دارد، فراخوانی می‌کند.

۱۰ برهم‌کنش بین سازوکارهای امنیتی

اغلب این چنین است که چندین خدمت امنیتی مختلف برای یک نمونه از ارتباطات مورد نیاز است. این الزام را می‌توان با استفاده از یک سازوکار امنیتی که چندین خدمت امنیتی را فراهم ساخته و یا با استفاده از چندین سازوکار امنیتی به طور همزمان مرتفع کرد.

همزمانی استفاده از چندین سازوکار امنیتی، یکی از مواردی است که در آن سازوکارها طوری با یکدیگر برهم‌کنش دارند که می‌توانند به‌وسیله‌ی یک مهاجم مورد سوء استفاده قرار گیرند. این بدان معنی است که سازوکارهایی که یک سطح قابل قبول از امنیت را ایجاد می‌کنند، هنگامی که به تنهایی مورد استفاده قرار گیرند ممکن است نسبت به زمانی که به صورت ترکیبی با سایر سازوکارها مورد استفاده قرار می‌گیرند، آسیب‌پذیرتر باشند. این به طور معمول از مواردی است که دو سازوکار امنیتی می‌توانند به روش‌های مختلفی با یکدیگر ترکیب شوند. آسیب‌پذیری‌های سازوکارهای ترکیب شده با توجه به روش ترکیب شدنشان با یکدیگر متفاوت است.

یک مورد خاص و مهم از برهم‌کنش سازوکارها با یکدیگر زمانی رخ می‌دهد که دو سازوکار رمزنگاری با یکدیگر ترکیب می‌شوند (به عنوان مثال سازوکار یکپارچگی با یک سازوکار محرمانگی یا یک سازوکار انکارناپذیری با یک سازوکار محرمانگی). خصوصیت‌های امنیتی سازوکارهای ترکیب شده به ترتیب اعمال تبدیلات رمزنگاری بستگی دارد.

به طور کلی، هنگامی که از الگوریتم‌های رمزنگاشتی نامتقارن استفاده می‌شود، عمل انکارناپذیری یا یکپارچگی باید بر روی متن ساده اعمال شده و سپس داده‌های امضا شده یا مهر شده‌ی حاصل باید رمزگذاری شوند.

نمونه‌ای از مواردی که در آن اعمال دو خدمت به صورت معکوس (یعنی اول محرمانگی) ضروری است، زمانی است که خدمات بین هستارهای مختلف اعمال شده و یک هستار نیازمند آن است بتواند بدون این که بدان اجازه‌ی دانستن متن ساده داده شود، یکپارچگی متن رمزشده را درستی‌سنجی کند. این موقعیت ممکن است در سامانه‌های سامان‌دهی[1] پیام رخ دهد. جایی که یک عامل انتقال پیام ممکن است نیاز داشته باشد یکپارچگی و مبدأ پیام‌ها را بدون این‌که اجازه‌ی دانستن متن ساده پیام را داشته باشد، درستی‌سنجی کند.

استفاده از خدمات محرمانگی و یکپارچگی به ترتیب معکوس این خطر را به دنبال دارد که خدمت یکپارچگی نتواند انکارناپذیری را پشتیبانی کند. اگر همگی این سه خدمت مد نظر باشند و ترتیب معکوس یکپارچگی و محرمانگی ضروری باشد، آنگاه امکان اعمال دو سازوکار یکپارچگی یکی قبل و یکی بعد از سازوکار محرمانگی وجود دارد. نمونه‌ای از این موقعیت در سامانه‌های سامان‌دهی پیام اتفاق می‌افتد. اگر محرمانگی فراهم شده باشد، آنگاه دو امضای دیجیتالی متفاوت را می‌توان در پیام جاسازی کرد (یکی از روی متن رمزشده برای استفاده به‌وسیله‌ی عامل انتقال پیام محاسبه شده و یکی از روی متن ساده محاسبه می‌شود تا انکارناپذیری مبدأ را برای دریافت کننده مهیا سازد).

۱۱ دسترس‌پذیری و انکار خدمت

انکار خدمت، زمانی اتفاق می‌افتدکه یک خدمت به کمتر از آن سطحی که مورد نیاز است کاهش یابد که این امر شامل از دسترس خارج شدن خدمت نیز می‌شود. این انکار خدمت ممکن است بر اثر یک حمله‌ی عمدی یا اتفاقاتی مانند یک طوفان یا زمین لرزه اتفاق بیافتد. دسترس‌پذیری شرایطی است که در آن هیچ انکاری از خدمت یا کاهش کیفیت ارتباطی وجود ندارد.

همواره امکان جلوگیری از انکار خدمت وجود ندارد. خدمات امنیتی می‌توانند برای تشخیص ممانعت مورد استفاده قرار گیرند به طوری که بتوان اقدامات متقابل مناسب اتخاذ کرد. این تشخیص ممکن است نتواند مشخص کند که انکار خدمت بر اثر حمله رخ داده یا نتیجه‌ی شرایطی اتفاقی بوده است. یک خط مشی امنیتی خاص ممکن است نیازمند آن باشد که زمانی که یک انکار خدمت تشخیص داده می‌شود، باید سابقه‌ی آن (برای اهداف ممیزی) ثبت شده و یک هشدار به پردازشگر هشدار ارسال شود.

هنگامی که یک شرایط انکار خدمت تشخیص داده می‌شود، ممکن است از خدمات امنیتی نیز برای بازسازی و بازگرداندن آن به سطحی قابل قبول از خدمت استفاده شود. این تشخیص و عملیات اصلاحی[2] ممکن است، استفاده از خدمات امنیتی و خدمات غیرامنیتی (مانند مسیریابی دوباره ترافیک روی سایر پیوندها، سو دادن به تسهیلات ذخیره‌سازی پشتیبان، یا آوردن پردازش‌گرهای پشتیبان بر خط[3]) نیز شامل شود.

1 - Handling systems
2 - Corrective actions
3 - On-line

بسیاری از انواع مختلف خدمات مد نظر حملات انکار خدمت قرار دارند و سازوکارهایی که برای جلوگیری از آن‌ها مورد استفاده قرار می‌گیرند ممکن است برای هر نوع از کاربرد محافظت شونده‌ای، متفاوت باشند. این بدان معنی است که امکان دسته‌بندی سازوکارهای محافظتی در برابر انکار خدمت به طور کلی وجود ندارد و از این رو چارچوب‌های کاری امنیتی، آن‌ها را بیشتر مورد توجه قرار نمی‌دهند.

۱۲ سایر الزامات

ممکن است الزامات امنیتی بیشتری نسبت به آنچه در این چارچوب‌های کاری توضیح داده شده است مورد نیاز باشند (مانند الزامات امنیتی فیزیکی و شخصی). تعریف خدمات امنیتی برای پشتیبانی از این الزامات خارج از محدوده‌ی این استاندارد ملی است. استفاده از الزامات امنیتی بیشتر ممکن است حتی نیاز به استفاده از برخی از خدمات امنیتی بیان شده در این چارچوب کاری را مرتفع سازد.

پیوست الف

مثال‌هایی از سازوکارهای محافظتی برای گواهی‌های امنیتی (اطلاعاتی)

یک تهدید بالقوه که شامل گواهی‌های امنیتی است، تهدیدی است که یک مهاجم به نادرستی ادعا می‌کند که هستاری است که آن گواهی امنیتی به آن اشاره می‌کند. به چنین استفاده‌ی غیرمجازی از یک گواهی امنیتی به‌عنوان دزدی یک گواهی امنیتی ارجاع می‌شود.

این تهدید می‌تواند هم یک تهدید نفوذگر داخلی و هم یک تهدید بیرونی باشد. تهدید بیرونی تهدیدی است که مهاجم ممکن است یک گواهی امنیتی را با شنود[1] از ارتباطاتی که دیگر در آن‌ها وجود ندارد، به‌دست آورد. یک تهدید نفوذگر داخلی تهدیدی است که یک هستار که نیازی قانونی (به عنوان مثال به منظور فراهم کردن اطلاعات امنیتی یک هستار که با آن در ارتباط است) به کسب یک گواهی دارد ممکن است به صورت نادرست خود را هستاری که گواهی امنیتی به آن مربوط می‌شود، معرفی کند.

یک گواهی امنیتی ممکن است در برابر دزدی محافظت شود که این کار با استفاده‌ی مستقیم از خدمات امنیتی ارتباطات در OSI و یا با استفاده از روش‌های محافظتی جایگزین که نیازمند پارامترهای بیشتر داخلی و خارجی است، انجام می‌شود.

یک سازوکار محافظتی برای گواهی‌های امنیتی گفته می‌شود که از واگذاری[2] پشتیبانی می‌کند اگر یک هستار که حق استفاده از گواهی امنیتی را دارد، حق خود را به هستار دیگری واگذار کند. برخی از سازوکارهای توضیح داده شده در این پیوست از واگذاری پشتیبانی می‌کنند.

الف-۱ محافظت با استفاده از یک خدمت امنیتی ارتباطات در OSI

مقابله با یک تهدید دزدی از سوی یک مهاجم بیرونی هنگامی که گواهی امنیتی بین هستارهای ارتباطی انتقال می‌یابد ممکن است با استفاده از یک خدمت محرمانگی انجام شود.

الف-۲ محافظت با استفاده از یک پارامتر درونی گواهی‌های امنیتی

تعدادی از روش‌های جایگزین برای محافظت از گواهی‌های امنیتی در برابر دزدی وجود دارد. هر یک از این روش‌ها بر پارامتری درونی از گواهی و پارامترهای بیرونی مرتبط با آن متکی هستند.

در اینجا به روش‌های خاص مورد استفاده درون گواهی امنیتی اشاره می‌شود.

این روش‌ها عبارتند از:

- روش احراز هویت؛
- روش کلید خصوصی؛

1 - Eavesdrop
2 - Delegation

- روش کلید عمومی؛
- روش تابع یک سویه.

یک گواهی امنیتی ممکن است از ترکیبی از چندین روش از روش‌های فوق استفاده کند.

الف-۲-۱ روش احراز هویت

در این روش، پارامتر درونی، شناسه‌های تمیزدهنده‌ی هستارها هستند که اجازه‌ی استفاده از گواهی به آن‌ها داده شده است. پارامتر بیرونی، شناسه تمیزدهنده‌ی هستاری است که در تلاش است از گواهی استفاده کند. این پارامتر بیرونی به‌وسیله‌ی یک خدمت احراز هویت فراهم می‌شود. گواهی ممکن است شامل پارامترهای درونی بیشتری از جمله شماره سری گواهی احراز هویتی باشد که در فرآیند احراز هویت از آن استفاده می‌شود.

روش احراز هویت بیان شده در ذیل محافظت را برای گواهی امنیتی به دنبال دارد:

- این روش استفاده از گواهی امنیتی را به هستارهایی محدود می‌کند که شناسه‌های آن‌ها در گواهی امنیتی وجود دارد.

این روش به یک کاربر مجاز گواهی اجازه‌ی انتقال حق استفاده‌ی خود از گواهی را به هستاری دیگر نمی‌دهد. چرا که هستارهایی که ممکن است از گواهی استفاده کنند ثابت بوده و در زمان ایجاد گواهی مشخص می‌شوند. به این معنی که این روش از واگذاری پشتیبانی نمی‌کند.

الف-۲-۲ روش کلید سرّی

در این روش، تمامی گواهی با استفاده از یک الگوریتم رمزنگاشتی متقارن رمزگذاری می‌شود. پارامتر بیرونی در این روش کلید سرّی است که برای رمزگذاری مورد استفاده قرار می‌گیرد.

روش کلید سرّی محافظت ذیل را برای گواهی امنیتی فراهم می‌کند:

- این روش استفاده از گواهی را به هستارهایی محدود می‌کند که مقدار کلید سرّي را می‌دانند (و در نتیجه قادر به رمزگشایی گواهی رمزگذاری شده هستند).

این روش از واگذاری پشتیبانی می‌کند چرا که یک کاربر مجاز گواهی می‌تواند حق استفاده از گواهی خود را به هستار دیگری بدهد، که این کار را می‌تواند با دادن کلید سرّی و یا دادن گواهی رمزگشایی‌شده به آن هستار انجام دهد.

الف-۲-۳ روش کلید عمومی

در این روش پارامتر درونی یک کلید عمومی است. پارامتر بیرونی کلید خصوصی معادل است.

روش کلید عمومی محافظت بیان شده در ذیل را برای گواهی امنیتی به دنبال دارد:

- این روش استفاده از گواهی امنیتی را به هستارهایی محدود می‌کند که کلید خصوصی را می‌دانند (و در نتیجه قادرند امضای دیجیتالی را با استفاده از کلید خصوصی محاسبه کنند).

این روش از واگذاری پشتیبانی می‌کند. چرا که یک کاربر مجاز گواهی ممکن است با دادن کلید خصوصی به هستار دیگری، حق خود در استفاده از گواهی را به آن هستار واگذار کند.

الف-۲-۴ روش تابع یک سویه

در این روش پارامتر درونی نتیجه‌ی اعمال یک تابع یک سویه بر پارامتر بیرونی است. پارامتر درونی به عنوان

یک کلید محافظت شده شناخته می‌شود. در حالی که پارامتر بیرونی به عنوان یک کلید کنترلی شناخته می‌شود.

روش تابع یک سویه محافظت بیان شده در ذیل را برای گواهی امنیتی به دنبال دارد:

- این روش استفاده از گواهی امنیتی را به هستارهایی محدود می‌کند که مقدار کلید کنترلی را می‌دانند (و در نتیجه قادرند با افشای مقدار کلید کنترلی ثابت کنند که مقدار آن را می‌دانند).

این روش از واگذاری پشتیبانی می‌کند. چرا که یک کاربر مجاز گواهی ممکن است با دادن کلید کنترلی به هستار دیگری، حق خود در استفاده از گواهی را به آن هستار واگذار کند.

الف-۳ محافظت از پارامترهای درونی و بیرونی در حال انتقال

چهار مورد باید مورد توجه قرار گیرد که عبارتند از:

- انتقال پارامتر درونی به هستار مرجع مرجع قبل از آنکه گواهی ایجاد شود. این مورد در صورتی مورد نیاز است که پارامترهای درونی و بیرونی به‌وسیله‌ی هستار مرجع ایجاد نشده باشد.
- انتقال پارامتر بیرونی از هستار مرجع مرجع پس از آنکه گواهی ایجاد می‌شود. این مورد در صورتی مورد نیاز است که پارامترهای درونی و بیرونی به‌وسیله‌ی هستار مرجع مرجع ایجاد شده باشد.
- انتقال پارامتر بیرونی بین هستارها هنگامی که حق استفاده از گواهی داده شود.
- انتقال پارامتر بیرونی بین هستارها هنگامی که حق استفاده از گواهی به هستار دیگری واگذار می‌شود.

الف-۳-۱ انتقال پارامترهای درونی به هستار مرجع امنیتی مرجع

در روش احراز هویت، روش کلید عمومی و روش تابع یک سویه، پارامتر درونی ممکن است به هستار مرجع امنیتی قبل از این‌که گواهی امنیتی ایجاد گردد، منتقل شود. پارامتر درونی باید از نظر یکپارچگی در حالی که به هستار مرجع امنیتی انتقال می‌یابد، محافظت شود.

در روش کلید سرّی، پارامتر بیرونی (یعنی کلید سرّی) ممکن است قبل از ایجاد شدن گواهی به هستار مرجع امنیتی فرستاده شود. این انتقال نیازمند آن محافظت برای تامین یکپارچگی و محرمانگی است.

الف-۳-۲ انتقال پارامترهای بیرونی به هستارها

در روش احراز هویت، پارامتر بیرونی (هویت کاربر گواهی) به‌وسیله‌ی یک سازوکار احراز هویت فراهم می‌شود. در روش کلید سرّی و روش تابع یک سویه، پارامتر بیرونی باید بین هستارها هنگامی منتقل شود که از گواهی استفاده می‌شود. این کار استفاده از گواهی امنیتی را به آن‌هایی محدود می‌کند که مقدار درست کلید سرّی یا کلید کنترلی را می‌دانند. پارامتر بیرونی باید هنگام انتقال بین هستارها از نظر محرمانگی محافظت شود.

یک تفاوت بین این دو روش در آن است که به هنگام استفاده از روش کلید سرّی، ضروری است که مقدار پارامتر بیرونی قبل از درستی‌سنجی مقدار وارسی رمزنگاشتی گواهی امنیتی افشا شود. در حالی که در روش تابع یک سویه، مقدار وارسی گواهی امنیتی قبل از این‌که پارامتر بیرونی افشا شود، درستی‌سنجی می‌شود.

در روش کلید خصوصی، پارامتر بیرونی نیازی به منتقل شدن بین هستارها هنگام استفاده از گواهی ندارد. چرا که یک هستار می‌تواند بدون این‌که مقدار آن را افشا کند (با ساخت یک امضای دیجیتالی) ثابت کند که

مقدار کلید خصوصی را می‌داند. با این روش، پارامتر بیرونی (کلید خصوصی) تنها زمانی نیازمند منتقل شدن است که استفاده از گواهی به هستار دیگری واگذار می‌شود. کلید خصوصی باید هنگام انتقال بین هستارها از نظر محرمانگی محافظت شود.

الف-۴ استفاده از گواهی‌های امنیتی به‌وسیله‌ی یک یا گروهی از هستارها

روش‌های محافظتی توضیح داده شده‌ی فوق، ممکن است برای محدود کردن استفاده از یک گواهی امنیتی به یک هستار خاص یا گروهی از هستارها، مورد استفاده قرار گیرند که عبارتند از:

- یک گواهی امنیتی ممکن است به یک هستار خاص مقید شود. کلید سرّي، کلید خصوصی یا کلید کنترلی به صورت رمزگذاری شده به یک هستار فرستاده می‌شوند و شناسه تمیزدهی یا صفات امنیتی هستار در گواهی امنیتی ظاهر می‌شود.
- یک گواهی امنیتی ممکن است به یک گروه خاص از هستارها مقید شود. کلید سرّي، کلید خصوصی یا کلید کنترلی به صورت رمزگذاری شده به اعضای آن گروه فرستاده شود و شناسه تمیزدهی یا خواص امنیتی گروه در گواهی امنیتی ظاهر می‌شوند. در این روش، هر عضو از گروه از گواهی امنیتی استفاده می‌کند.

الف-۵ پیوند یک گواهی امنیتی به دسترسی‌ها

گواهی‌های امنیتی را می‌توان برای کنترل دسترسی مورد استفاده قرار داد. مهم این است که یک پیوند امن بین گواهی امنیتی و درخواست‌های پشتیبانی شده‌ی دسترسی برقرار شود. اگر چنین پیوند امنی وجود ندارد، آنگاه گواهی امنیتی در برابر حمله‌ی دست‌کاری که مهاجم یک رونوشت از اصل گواهی امنیتی را به همراه یک درخواست دسترسی جعل شده می‌فرستد، آسیب‌پذیر است.

از این حمله می‌توان با استفاده از خدمت یکپارچگی برای الحاق گواهی امنیتی، پارامتر بیرونی و درخواست دسترسی به همدیگر، جلوگیری کرد.

هنگامی که از روش احراز هویت استفاده می‌شود، این اتصال را می‌توان با پیوند تبادل احراز هویت با یک سازوکار یکپارچگی انجام داد. این موضوع در چارچوب کاری احراز هویت توضیح داده می‌شود (توصیه‌نامه ITU-T X811 | ISO/IEC 10181-2 را مشاهده کنید).

هنگامی که از روش کلید سرّی استفاده می‌شود، این ملحق‌سازی را می‌توان با قرار دادن یک کلید برای سازوکار یکپارچگی درون بدنه‌ی گواهی امنیتی و استفاده از این کلید برای برقراری درخواست دسترسی، انجام داد. به جای این کار، کلید سرّی (یا نوعی تغییریافته از آن) ممکن است به عنوان کلید برای یک سازوکار یکپارچگی مورد استفاده قرار گیرد.

یادآوری- استفاده از کلید رمزنگاری یکسان برای هر دو سازوکار یکپارچگی و محرمانگی ممکن است منجر به وقوع برخی حملات شود. برای محافظت در برابر این تهدید، انواع دیگری از کلید ممکن است مورد استفاده قرار گیرند. یک نمونه‌ی دیگر از یک کلید رمزنگاری شده یک کلید رمزنگاری دیگر است که از روی کلید اولیه به‌دست آمده و با آن برابر نیست.

هنگامی که از روش تابع یک سویه استفاده می‌شود، این اتصال را می‌توان با استفاده از کلید کنترلی به عنوان یک کلید در یک سازوکار یکپارچگی مبتنی بر توابع یک سویه، انجام داد.

هنگامی که از روش کلید عمومی استفاده می‌شود، این اتصال را می‌توان با استفاده از کلید عمومی برای اختصاص درخواست‌های دسترسی، انجام داد.

با استفاده از تمامی این روش‌ها، اتصال گواهی امنیتی، پارامتر بیرونی و درخواست دسترسی را می‌توان با استفاده از یک خدمت یکپارچگی نیز که به عنوان قسمتی از یک خدمت ارتباطی در OSI قرار داده شده، انجام داد.

پیوست ب

کتاب‌نامه

(اطلاعاتی)

- توصیه‌نامه (1995) ITU-T X.811 | ISO/IEC 10181-2: 1996، فناوری اطلاعات - اتصال متقابل سامانه‌های باز-چارچوب‌های کاري امنیتی برای سامانه‌های باز: چارچوب کاري احراز هویت.
- توصیه‌نامه (1995) ITU-T X.812 | ISO/IEC 10181-3: 1996، فناوری اطلاعات-اتصال متقابل سامانه‌های باز-چارچوب‌های کاري امنیتی برای سامانه‌های باز: چارچوب کنترل دسترسی.
- توصیه‌نامه (1993) ITU-T X.509 | ISO/IEC 9594-8: 1995، فناوری اطلاعات-اتصال متقابل سامانه‌های باز-فهرست راهنما: چارچوب کاري احراز هویت.
- استاندارد ISO/IEC 11770-1، فناوری اطلاعات-روش‌های امنیتی-مدیریت کلید-بخش ۱: چارچوب مدیریت کلید.
- استاندارد ISO/IEC 9798-1: 1991، فناوری اطلاعات-روش‌های امنیتی-سازوکارهای احراز هویت هستار-بخش ۱: طرح کلی.