استاندارد ملی ایران

۱۶۲۷۴-۲

چاپ اول

اردیبهشت ۱۳۹۲

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران

Iranian National Standardization Organization

INSO
16274-2

1st. Edition
May.2013

سامانه‌های پردازش اطلاعات- اتصال متقابل سامانه‌های باز- مدل مرجع پایه- قسمت ۲: معماری امنیتی

Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

ICS: 35.100.01

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

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

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

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

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

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

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

کمیسیون فنی تدوین استاندارد

«سامانه‌های پردازش اطلاعات – اتصال متقابل سامانه‌های باز – مدل مرجع پایه – قسمت ۲: معماری امنیتی»

رئیس:	**سمت و/ یا نمایندگی**
میرزایی رضایی، طیبه (کارشناسی‌ارشد فیزیک)	رییس اداره تدوین استانداردها و نظارت بر فرآیند سرویس‌ها سازمان فناوری اطلاعات ایران
دبیر:	
میراسکندری، سید محمدرضا (کارشناسی مهندسی کامپیوتر نرم افزار)	مدیر کل خدمات ارزش افزوده سازمان فناوری اطلاعات ایران
اعضاء: (اسامی به ترتیب حروف الفبا)	
بختیاری، شیرین (کارشناسی مهندسی برق کنترل)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
جمیل پناه، ناصر (کارشناسی‌ارشد مدیریت)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سعیدی، عذرا (کارشناسی‌ارشد مهندسی برق-مخابرات)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
سلطانی حقیقت، الهه (کارشناسی مهندسی برق مخابرات)	کارشناس سازمان فناوری اطلاعات ایران
عبداللهی ازگمی، محمد (دکترای مهندسی کامپیوتر-نرم‌افزار)	استادیار دانشگاه علم و صنعت ایران
عسکرزاده، مجید (کارشناسی‌ارشد مهندسی کامپیوتر)	کارشناس موسسه تحقیقات ارتباطات و فناوری اطلاعات
فرهاد شیخ احمد، لیلا (کارشناسی‌ارشد مهندسی کامپیوتر نرم افزار)	کارشناس تدوین استاندارد سازمان فناوری اطلاعات ایران
فولادیان، مجید (کارشناسی‌ارشد مهندسی برق-مخابرات)	مشاور سازمان فناوری اطلاعات ایران
فیاضی، مهدی (کارشناسی مهندسی برق الکترونیک)	کارشناس مسؤول تدوین استاندارد و امنیت شبکه سازمان فناوری اطلاعات

قسمتی، سیمین
(کارشناسی‌ارشد فناوری اطلاعات)
کارشناس سازمان فناوری اطلاعات ایران

مجاهدی، الناز
(کارشناسی مهندسی کامپیوتر نرم‌افزار)
نماینده دانشگاه علم و صنعت ایران

معروف، سینا
(کارشناسی مهندسی کامپیوتر سخت‌افزار)
کارشناس سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «سامانه‌های پردازش اطلاعات – اتصال متقابل سامانه‌های باز – مدل مرجع پایه – قسمت ۲: معماری امنیتی» که پیش‌نویس آن درکمیسیون‌های مربوط به وسیله سازمان فناوری اطلاعات تهیه و تدوین شده و در اجلاس دویست و شصت و یکمین اجلاس کمیته‌ی ملی استاندارد رایانه و فرآوری داده مورخ ۱۳۹۱/۱۲/۶ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده‌ی ۳ قانون اصلاح قوانین و مقررات سازمان استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به‌عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در 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 7498-2:1989, Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture

مقدمه

این استاندارد یکی از مجموعه استانداردهای ملی ایران به شماره ۱۶۲۷۴ است.خانواده استاندارد بین المللی ISO 7498، مدل مرجع پایه[1] اتصال متقابل سامانه‌های باز (OSI)[2] را توصیف می کند. استاندارد بین المللی ISO 7498-2 چارچوبی را برای هماهنگ کردن تدوین استانداردهای موجود و آتی برای اتصال متقابل سامانه‌ها ایجاد می‌کند.

هدف OSI آن است که اتصال متقابل سامانه‌های رایانه‌ای ناهمگون[3] را مجاز کند، طوری که ارتباط سودمند بین فرایندهای کاربردی[4] قابل حصول شود. در زمان‌های گوناگون، باید کنترل‌های امنیتی برای محافظت از اطلاعات مبادله‌شده بین فرایندهای کاربردی ایجاد شود. چنین کنترل‌هایی باید هزینه به‌دست آوردن یا تغییر داده‌ها را از ارزش بالقوه برای انجام آن به مراتب بیشتر کرده، یا زمان مورد نیاز برای به‌دست آوردن داده‌ها را از ارزش داده‌های از دست رفته به مراتب بیشتر کنند.

استاندارد بین المللی ISO 7498-2، عناصر معماری مرتبط به امنیت عمومی[5] را تعریف می‌کند که می‌تواند به‌طور مناسب در شرایطی به‌کار رود که محافظت از ارتباط بین سامانه‌های باز مورد نیاز است. این استاندارد در چارچوب مدل مرجع، راهنماها و محدودیت‌های در جهت بهبود استانداردهای موجود یا تدوین استانداردهای جدید در زمینه OSI[6] به‌منظور اجازه دادن ارتباطات امن و در نتیجه فراهم کردن یک رهیافت سازگار برای امنیت در OSI به‌کار گرفته می‌شود.

داشتن پیش‌زمینه‌ای[7] در امنیت برای فهم این سند مفید خواهد بود. به خواننده‌ای که به خوبی با امنیت آشنایی ندارد توصیه می‌شود که ابتدا پیوست-الف را مطالعه کند.

استاندارد بین المللی ISO 7498-2، مدل مرجع پایه را به‌منظور پوشش جنبه‌های امنیتی که عناصر معماری عمومی پروتکل‌های ارتباطاتی هستند، تعمیم می‌دهد، اما شامل موارد مورد بحث در مدل مرجع پایه نیست.

1 - Basic Reference Model
2 - Open Systems Interconnection (OSI)
3 - Heterogeneous
4 - Application processes
5 - General security-related architectural elements
6 - Context
7 - Background

سامانه‌های پردازش اطلاعات - اتصال متقابل سامانه‌های باز - مدل مرجع پایه - قسمت ۲: معماری امنیتی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین موارد زیر است:

الف- یک توصیف کلی از خدمات امنیتی و سازوکارهای مرتبط فراهم می‌کند که ممکن است به وسیله مدل مرجع فراهم شده باشند؛ و

ب- موقعیت‌هایی را درون مدل مرجع تعریف می‌کند که ممکن است خدمات و سازوکارها در آن‌جا فراهم شده باشند.

این استاندارد، حوزه کاربرد استاندارد ISO 7498 را تعمیم داده، تا ارتباطات امن بین سامانه‌های باز را پوشش دهد.

خدمات و سازوکارهای امنیتی پایه و جای‌گذاری‌های مناسب آن‌ها برای همه لایه‌ها در مدل مرجع پایه شناسایی شده است. به‌علاوه، ارتباطات معماری خدمات و سازوکارهای امنیتی مدل مرجع پایه شناسایی شده است. تمهیدات[1] امنیتی اضافی ممکن است در سامانه‌های پایانی[2]، نصب‌ها[3] و سازمان‌ها مورد نیاز باشند. این ابزارها در زمینه‌های کاربردی مختلف به‌کارگیری می‌شوند. تعریف خدمات امنیتی مورد نیاز برای پشتیبانی چنین ابزارهای امنیتی اضافی، خارج از حوزه‌ی این استاندارد است.

کارکردهای امنیتی OSI تنها به آن جنبه‌های قابل مشاهده‌ی یک مسیر ارتباطی مربوط می‌شوند که در آن به سامانه‌های پایانی اجازه دست‌یابی به انتقال امن اطلاعات بین خود را می‌دهد. امنیت OSI به ابزارهای امنیتی مورد نیاز در سامانه‌های پایانی، نصب‌ها و سازمان‌ها مربوط نمی‌شود، به جز جاهایی که این موارد مستلزم انتخاب و قراردادن خدمات امنیتی قابل مشاهده در OSI است. این جنبه‌های امنیتی آخری مجاز به استانداردسازی هستند اما نه در حوزه‌ی استانداردهای OSI.

استاندارد مواردی را به مفاهیم و اصول تعریف شده در سری خانواده استاندارد ۷۴۹۸ می‌افزاید؛ ولی تغییری در آن‌ها نمی‌دهد. این استاندارد نه یک مشخصات پیاده‌سازی و نه مبنایی برای ارزیابی انطباق پیاده‌سازی‌های واقعی است.

۲ مراجع الزامی

۲-۱ استاندارد بین المللی ISO 7498-2 : *سامانه‌های پردازش اطلاعات- اتصال سامانه‌های باز- قسمت ۴: چارچوب مدیریتی*

1 - Measure
2 - End-Systems
3 - Installations

2-2 ISO 7498 Information processing systems, Open Systems Interconnection, Basic Reference Model.

2-3 ISO 7498/Add.l Information processing Systems, - Open Systems Interconnection, Basic Reference Model
Addendum 1: Connectionless-mode transmission.

2-4 ISO 8648 Information processing systems, Open Systems Interconnection, Internal organization of the Network Layer

۳ اصطلاحات و تعاریف

در این استاندارد اصطلاحات و تعاریف زیر به‌کار می‌رود:

۳-۱ این استاندارد بر پایه مفاهیم تدوین داده شده در استاندارد ISO 7498 بنا شده و از اصطلاحات زیر استفاده می‌کند:

اصطلاح	کوته‌نوشته	معادل
اتصال لایه N	(N)-اتصال	(N)-connection
ارسال داده لایه N	(N)-ارسال داده	(N)-data-transmission
هستار لایه N	(N)-هستار	(N)-entity
تسهیلات لایه N	(N)-تسهیلات	(N)-facility
لایه N	(N)-لایه	(N)-layer
سامانه باز		Open System
هستارهای همتا		Peer entities
پروتکل لایه N	(N)-پروتکل	(N)-protocol
واحد داده‌ای پروتکل لایه N	(N)-واحد داده‌ی پروتکل	(N)-protocol-data-unit
رله لایه N	(N)-رله	(N)-relay
مسیریابی		Routing
ترتیب‌دهی		Sequencing
خدمت لایه N	(N)-خدمت	(N)-service
واحد داده‌ای خدمت لایه N	(N)-واحد داده‌ی خدمت	(N)-service-data-unit
داده‌های کاربر لایه N	(N)-داده‌ی کاربر	(N)-user-data
زیرشبکه		Subnetwork
منبع OSI		OSI resource
نحو انتقال		Transfer syntax

۳-۲ این استاندارد از اصطلاحات زیر که از استانداردهای بین‌المللی مربوطه استخراج شده‌اند استفاده می‌کند:

اصطلاح	استاندارد

حالت انتقال بی‌اتصال	(ISO 7498/Add.l)
سامانه پایانی	(ISO 7498)
کارکرد رله و مسیریابی	(ISO 8648)
UNITDATA	(ISO 7498)
پایگاه اطلاعات مدیریت (MIB)	(استاندارد ۴-۷۴۹۸)

به‌علاوه، کوته‌نوشت‌های زیر نیز مورد استفاده قرار می‌گیرند:

اتصال متقابل سامانه‌های باز	Open System Interconnection	OSI
واحد داده خدمت	Service Data Unit	SDU
پایگاه اطلاعات مدیریت امنیت	Security Management Information Base	SMIB
پایگاه اطلاعات مدیریت	Management Information Base (MIB)	MIB

۳-۳ با توجه به هدف این استاندارد، تعاریف زیر به‌کار برده می‌شوند:

۱-۳-۳

کنترل دسترسی[1]

جلوگیری از استفاده‌ی غیرمجاز از یک منبع است که شامل جلوگیری از استفاده از یک منبع به روش غیرمجاز است.

۲-۳-۳

فهرست کنترل دسترسی[2]

فهرستی از هستارها به همراه حقوق دسترسی هر یک از آن‌ها که اجازه‌ی دسترسی مجاز به یک منبع را دارند.

۳-۳-۳

پاسخ‌گویی[3]

خصوصیتی که اطمینان می‌دهد که کنش‌های[4] یک هستار می‌تواند به‌طور یکتا[5] به آن هستار ردیابی[6] شود.

۴-۳-۳

تهدید فعال[7]

تهدید، یک تغییر غیرمجاز عمدی به حالت سامانه است.

1 - Access Control
2 - Access Control List
3 - Accountability
4 - Actions
5 - Uniquely
6 - Traced
7 - Active threat

یادآوری- مثال‌هایی از تهدیدات فعال مرتبط با امنیت عبارتند از: تغییر پیام‌ها، بازپخش[1] پیام‌ها، درج پیام‌های جعلی، خود را به یک هستار مجاز دگرنمایی[2] کردن و انکار خدمت[3].

۵-۳-۳

ممیزی[4]

به بند ممیزی امنیت مراجعه شود.

۶-۳-۳

دنباله‌ی ممیزی[5]

به بند دنباله‌ی ممیزی امنیت مراجعه شود.

۷-۳-۳

احراز هویت[6]

به بندهای احراز هویت مبدأ داده‌ها و احراز هویت هستارهای همتا مراجعه شود.

یادآوری- دراین استاندارد، عبارت «احراز هویت» در رابطه با «یکپارچگی داده‌ها» مورد استفاده قرار نمی‌گیرد در عوض از عبارت «یکپارچگی داده‌ها» استفاده می‌شود.

۸-۳-۳

اطلاعات احراز هویت[7]

اطلاعاتی که برای ایجاد اعتبار هویت ادعا شده مورد استفاده قرار می‌گیرند.

۹-۳-۳

تبادل احراز هویت[8]

سازوکار به‌کار رفته به‌منظور حصول اطمینان از هویت یک هستار با استفاده از تبادل اطلاعات است.

۱۰-۳-۳

مجازشناسی[9]

اعطای حقوق که شامل اعطای دسترسی مبتنی بر حقوق دسترسی است.

1 - Replay
2 - Masquerade
3 - Denial of Service
4 - Audit
5 - Audit trail
6 - Authentication
7 - Authentication information
8 - Authentication exchange
9 - Authorization

۱۱-۳-۳

دسترس‌پذیری[1]

خصوصیت در دسترس بودن و قابل استفاده بودن در قبال درخواست به‌وسیله یک هستار مجاز است.

۱۲-۳-۳

قابلیت[2]

نشانه‌ای[3] که به‌عنوان یک شناسه[4] برای یک منبع استفاده می‌شود، طوری‌که مالکیت آن نشانه به معنی داشتن حقوق دسترسی به منبع است.

۱۳-۳-۳

کانال[5]

یک مسیر انتقال اطلاعات است.

۱۴-۳-۳

متن رمزشده[6]

داده‌هایی که در نتیجه‌ی استفاده از رمزگذاری[7] تولید می‌شوند. محتوای معنایی داده‌های حاصله در دسترس نیست.

یادآوری- متن رمزگذاری شده، خود ممکن است ورودی رمزگذاری باشد، به طوری‌که خروجی ابررمزگذاری شده[8] تولید می‌شود.

۱۵-۳-۳

متن واضح[9]

داده‌های قابل فهم که محتوای معنایی آن‌ها در دسترس است.

۱۶-۳-۳

محرمانگی[10]

خصوصیتی برای نشان دادن اینکه اطلاعات در دسترس نبوده یا برای افراد، هستارها و فرآیندهای غیرمجاز افشاء نشده است.

---

1 - Availability
2 - Capability
3 - Token
4 - Identifier
5 - Channel
6 - Ciphertext
7 - Encipherment
8 - Super-enciphered
9 - Cleartext
10 - Confidentiality

۱۷-۳-۳

اعتبارنامه‌ها[1]

داده‌هایی که برای ایجاد هویت مورد ادعای هستار منتقل می‌شوند.

۱۸-۳-۳

تحلیل رمز[2]

تحلیل یک سامانه رمزنگاری و/یا ورودی‌ها و خروجی‌های آن برای استنتاج متغیرهای محرمانه و/یا داده‌های حساس شامل متن واضح.

۱۹-۳-۳

مقدار وارسی رمزنگاشتی[3]

اطلاعاتی که با انجام یک تبدیل[4] رمزنگاشتی (به بند رمزنگاری مراجعه شود.) بر روی واحد داده‌ای به‌دست آمده است.

یادآوری- به‌دست آوردن مقدار وارسی رمزنگاشتی ممکن است طی انجام یک یا چند مرحله حاصل شده و نتیجه‌ی یک تابع ریاضی با استفاده از کلید و یک واحد داده باشد. این اطلاعات به‌طور معمول برای بررسی یکپارچگی یک واحد داده‌ای به کار می‌رود.

۲۰-۳-۳

رمزنگاری[5]

سازوکاری[6] که دربرگیرنده اصول، وسایل و روش‌هایی برای یک تبدیل داده‌ای بوده به‌طوری که محتوای اطلاعاتی را مخفی و از تغییرات نامشخص و/یا استفاده‌ی غیرمجاز جلوگیری کند.

یادآوری- رمزنگاری روش‌هایی را مشخص می‌کند که در رمزگذاری و رمزگشایی[7] مورد استفاده قرار می‌گیرند. به حمله‌ای بر اصول، وسایل و روش‌های رمزنگاری، تحلیل رمز گفته می‌شود.

۲۱-۳-۳

یکپارچگی داده‌ها[8]

خصوصیتی که نشان‌دهنده‌ی آن است که داده‌ها با یک روش غیرمجاز تغییر داده نشده یا از بین نرفته‌اند.

---

1 - Credentials
2 - Cryptanalysis
3 - Cryptographic checkvalue
4 - Transformation
5 - Cryptography

۶- «discipline» - در این جمله، معنی «سازوکار» مناسب‌تر است.

7 - Decipherment
8 - Data integrity

۲۲-۳-۳

احراز هویت مبدأ داده‌ها[1]

تأیید[2] این‌که منبع (منشاء)[3] داده‌های دریافتی همان است که ادعا شده است.

۲۳-۳-۳

رمزگشایی

معکوس یک رمزگذاری برگشت‌پذیر است.

۲۴-۳-۳

رمزگشایی[4]

به بند ۳-۳-۲۳ مراجعه شود.

۲۵-۳-۳

انکار خدمت

جلوگیری از دسترسی مجاز به منابع یا به تأخیر انداختن عملیاتی که نسبت به زمان حساس هستند.

۲۶-۳-۳

امضای دیجیتالی[5]

داده‌هایی که به واحد داده اضافه شده یا یک تبدیل رمزنگاشتی (به بند **رمزنگاری** مراجعه شود.) از یک واحدداده‌ای که به دریافت‌کننده‌ی داده‌ها اجازه می‌دهد که منبع و یکپارچگی واحد داده‌ای را اثبات کرده و همچنین از جعل داده‌ها، برای مثال به‌وسیله دریافت‌کننده، محافظت کند.

۲۷-۳-۳

رمزبندی/رمز کردن

تبدیل رمزنگاشتی داده‌ها (به بند ۳-۳-۲۰ مراجعه شود.) برای تولید متن رمزشده.

یادآوری- در مواردی که فرآیند رمزگشایی معادل نتواند به سهولت اجرا شود ممکن است که رمزگذاری برگشت‌ناپذیر باشد.

۲۸-۳-۳

رمزگذاری[6]

به بند **رمزگذاری** مراجعه شود.

1 - Data origin authentication
2 - Corroboration
3 - Source
4 - Decryption
5 - Digital signature
6 - Encryption

۲۹-۳-۳

رمزگذاری انتها به انتها[1]

رمزگذاری داده‌های درون یا در سامانه پایانی مبدأ به‌همراه **رمزگشایی** متناظر آن که فقط درون یا در سامانه پایانی مقصد رخ می‌دهد. (به بند **رمزگذاری پیوند به پیوند** مراجعه شود.)

۳۰-۳-۳

خط مشی امنیتی مبتنی بر هویت[2]

یک خط مشی امنیتی مبتنی بر هویت و/یا صفات کاربران، گروهی از کاربران، یا هستارهایی که از جانب کاربران درحال فعالیت بوده و منابع/اشیایی که مورد دسترسی قرار می‌گیرند.

۳۱-۳-۳

یکپارچگی

به بند **یکپارچگی داده‌ها** مراجعه شود.

۳۲-۳-۳

کلید[3]

یک دنباله از نمادها که عملیات **رمزگشایی** و **رمزگذاری** را کنترل می‌کند.

۳۳-۳-۳

مدیریت کلید[4]

تولید، ذخیره، توزیع، حذف، بایگانی و کاربرد کلیدها مطابق یک **خط مشی امنیتی**.

۳۴-۳-۳

رمزگذاری پیوند به پیوند[5]

کاربرد مجزای **رمزگذاری** بر داده‌ها بر روی هر پیوند یک سامانه ارتباطی. (همچنین، به بند **رمزگذاری انتها به انتها** مراجعه شود.)

یادآوری – رمزگذاری پیوند به پیوند بر آن دلالت دارد که داده‌ها در هستارهای رله به شکل متن واضح خواهد بود.

۳۵-۳-۳

تشخیص فرابری[6]

سازوکاری جهت تشخیص اینکه آیا یک واحد داده تغییر یافته است یا خیر.

---

1 - End-to-end
2 - Identity-based security policy
3 - Key
4 - Key management
5 - Link-by-link
6 - Manipulation detection

۳۶-۳-۳

دگرنمایی

تظاهر یک هستار به اینکه هستار دیگری است.

۳۷-۳-۳

گواهی رسمی[1]

ثبت داده‌ها به وسیله یک طرف سوم قابل اعتماد[2] که اطمینان‌پذیری بعدی از دقت ویژگی‌های داده‌ها، نظیر محتوی، منشاء، زمان و تحویل آن را امکان‌پذیر می‌کند.

۳۸-۳-۳

تهدید غیرفعال[3]

تهدید یک افشای غیرمجاز اطلاعات بدون تغییر حالت سامانه است.

۳۹-۳-۳

کلمه عبور[4]

اطلاعات محرمانه احراز هویت که به‌طور معمول ترکیبی از یک رشته از نویسه‌ها است.

۴۰-۳-۳

احراز هویت هستار همتا[5]

تأیید اینکه یک هستار همتا در یک رابطه، همان است که ادعا کرده است.

۴۱-۳-۳

امنیت فیزیکی[6]

الزاماتی که برای فراهم‌سازی محافظت فیزیکی از منابع در برابر تهدیدات عمدی یا اتفاقی، مورد استفاده قرار می‌گیرند.

۴۲-۳-۳

خط مشی[7]

به بند **خط مشی امنیتی** مراجعه شود.

---

1 - Notarization
2 - Trusted third party
3 - Passive threat
4 - Password
5 - Peer-entity authentication
6 - Physical security
7 - Policy

۴۳-۳-۳

حریم خصوصی[1]

حق افراد برای کنترل و اثرگذاری[2] (نفوذ) بر اینکه چه اطلاعاتی مربوط به خودشان می‌تواند جمع‌آوری و ذخیره‌سازی گردد و اینکه به‌وسیله چه کسی و برای چه کسی آن اطلاعات می‌تواند افشا شود.

یادآوری- از آن‌جا که این عبارت به حق افراد مربوط می‌شود، نمی‌تواند خیلی دقیق باشد و از این رو از استفاده از آن باید اجتناب شود مگر به‌عنوان انگیزه‌ای برای ضروری دانستن امنیت.

۴۴-۳-۳

انکار[3]

امتناع یکی از هستارهای درگیر در یک ارتباط از پذیرش این‌که در تمام یا بخشی از ارتباط نقش داشته است.

۴۵-۳-۳

کنترل مسیریابی[4]

کاربرد قواعدی در طی فرآیند مسیریابی طوری‌که شبکه‌ها، پیوندها یا رله‌های خاصی انتخاب یا اجتناب شوند.

۴۶-۳-۳

خط مشی امنیتی مبتنی بر قاعده[5]

یک **خط مشی امنیتی** مبتنی بر قواعد کلی که برای همه کاربران اعمال می‌شود. این قواعد اغلب مبتنی بر مقایسه بین حساسیت منابع مورد دسترسی و دارا بودن صفات متناظر کاربران، گروهی از کاربران، یا هستارهایی است که از جانب کاربران عمل می‌کنند.

۴۷-۳-۳

ممیزی امنیت[6]

یک بازبینی و آزمایش مستقل رکوردها و فعالیت‌های سامانه، به‌منظور آزمودن کفایت کنترل‌های سامانه برای اطمینان از مطابقت آن‌ها با خط مشی‌های وضع شده و رویه‌های عملیاتی، برای تشخیص رخنه‌های امنیتی[7] و توصیه تغییرات معین در کنترل، خط مشی و رویه‌ها.

---

1 - Privacy
2 - Influence
3 - Repudiation
4 - Routing control
5 - Rule-based security policy
6 - Security audit
7 - Security breaches

۴۸-۳-۳

دنباله ممیزی امنیت[1]

داده‌های جمع‌آوری شده و به‌طور بالقوه استفاده شده برای سهولت یک ممیزی امنیتی است.

۴۹-۳-۳

برچسب امنیتی[2]

نشان‌های وابسته‌شده به یک منبع (که ممکن است یک واحد داده‌ای نیز باشد.) که آن را نام‌گذاری کرده یا خصوصیت‌های امنیتی آن منبع را مشخص می‌کنند.

یادآوری- نشانه‌گذاری و/یا وابسته‌سازی می‌تواند ضمنی یا صریح باشد.

۵۰-۳-۳

خط مشی امنیتی[3]

مجموعه‌ای از ابزارها برای فراهم کردن خدمات امنیتی (همچنین، به بند **خط مشی مبتنی بر هویت** و **مبتنی بر قاعده** مراجعه شود.)

یادآوری- یک خط مشی امنیتی کامل به طور الزامی بسیاری از نگرانی‌هایی که خارج از حوزه‌ی OSI است را مورد توجه قرار می‌دهد.

۵۱-۳-۳

خدمت امنیتی[4]

خدمتی که به‌وسیله یک لایه از سامانه‌های باز ارتباطی فراهم می‌شود که امنیت کافی سامانه‌ها یا انتقال‌های داده‌ای را تضمین می‌کند.

۵۲-۳-۳

محافظت فیلد انتخابی[5]

محافظت از فیلدهای خاصی از یک پیام که قرار است منتقل شود.

۵۳-۳-۳

حساسیت[6]

ویژگی یک منبع که دلالت بر ارزش یا اهمیت آن داشته و ممکن است شامل آسیب‌پذیری[7] آن نیز باشد.

---

1 - Security audit trail
2 - Security label
3 - Security policy
4 - Security service
5 - Selective field protection
6 - Sensitivity
7 - Vulnerability

۵۴-۳-۳

امضا[1]

به بند **امضای دیجیتالی** مراجعه شود.

۵۵-۳-۳

تهدید[2]

یک نقض بالقوه‌ی امنیت است.

۵۶-۳-۳

تحلیل ترافیک[3]

استنتاج اطلاعات از طریق مشاهده جریان‌های ترافیک. (حضور، فقدان، میزان، جهت و فراوانی)

۵۷-۳-۳

محرمانگی جریان ترافیک[4]

یک خدمت محرمانگی برای محافظت در برابر تحلیل ترافیک است.

۵۸-۳-۳

لت‌گذاری ترافیک[5]

تولید نمونه‌های جعلی از ارتباط، واحدهای داده‌ای جلعی و/یا داده‌های جعلی درون واحدهای داده‌ای است.

۵۹-۳-۳

کارکرد قابل اعتماد[6]

آنچه که با ملاحظه برخی معیارها استنباط[7] می‌شود که صحیح باشد، برای مثال از آنجایی که براساس یک خط مشی امنیتی ایجاد شده است.

۴ نشانه‌گذاری[8]

نشانه‌گذاری لایه‌ی مورد استفاده همان است که در سری خانواده استاندارد ۷۴۹۸ تعریف شده است.
اصطلاح «خدمت»، اگر توصیف دیگری ذکر نشده باشد، برای ارجاع به خدمت امنیتی استفاده می‌شود.

1 - Signature
2 - Threat
3 - Traffic analysis
4 - Traffic flow confidentiality
5 - Traffic padding
6 - Trusted functionality
7 - Perceived
8 - Notation

۵ توصیف کلی خدمات و سازوکارهای امنیتی

۵-۱ مرور کلی

خدمات امنیتی که در معماری امنیتی OSI قرار داده شده‌اند و سازوکارهایی که آن خدمات را پیاده‌سازی می‌کنند، در این بخش مورد بحث قرار می‌گیرند. خدمات امنیتی که در زیر توضیح داده شده‌اند، خدمات امنیتی پایه هستند. در عمل، این خدمات در لایه‌های مناسب و با ترکیب‌های مناسب و به‌طور معمول با خدمات و سازکارهای غیر OSI فراخوانی می‌شوند، تا خط مشی‌های امنیتی و/یا نیازهای کاربران را برآورده سازند. سازوکارهای امنیتی خاص می‌توانند برای پیاده‌سازی ترکیب‌هایی از این خدمات امنیتی پایه مورد استفاده قرار گیرند. محقق‌سازی‌های عملی[1] سامانه‌ها ممکن است ترکیب‌های خاصی از این خدمات امنیتی پایه را برای فراخوانی مستقیم پیاده‌سازی کنند.

۵-۲ خدمات امنیتی

آنچه در ادامه می‌آید به‌عنوان خدمات امنیتی در نظر گرفته شده‌اند که می‌توانند به‌طور بالقوه در چارچوب مدل مرجع OSI نیز فراهم شوند. خدمات احراز هویت نیازمند اطلاعات احراز هویتی هستند که دربرگیرنده ترکیبی از داده‌های ذخیره‌شده محلی و داده‌های انتقال داده‌شده (اعتبارنامه‌ها) برای تسهیل احراز هویت، هستند.

۵-۲-۱ احراز هویت

این خدمات برای احراز هویت یک هستار همتای ارتباطی و منبع داده‌ها به‌صورتی که در ادامه توضیح داده می‌شود، فراهم می‌شوند.

۵-۲-۱-۱ احراز هویت هستار همتا

این خدمت، زمانی که به وسیله (N)-لایه فراهم می‌شود، تأییدیه‌ای برای (N+1)-هستار فراهم می‌کند که همان است که (N+1)-هستار ادعا کرده است.

این خدمت برای استفاده در زمان ایجاد یا انجام مرحله انتقال داده‌ها در یک اتصال فراهم شده است تا هویت‌های یک یا چند هستار متصل به یک یا چند هستار دیگر را تأیید کند. این خدمت در زمانی که از آن استفاده می‌شود اطمینان می‌دهد که هیچ هستاری سعی در دگرنمایی خود به جای هستار دیگر نکرده و هیچ تکرار غیرمجازی از یک اتصال پیشین وجود ندارد. طرح‌های احراز هویت همتای یک طرفه و دو طرفه با یا بدون وارسی زنده بودن[2]، امکان‌پذیر بوده و می‌توانند درجه‌های متغیری از محافظت را فراهم کنند.

۵-۲-۱-۲ احراز هویت مبدأ داده‌ها[3]

این خدمت، زمانی که به وسیله (N)-لایه فراهم می‌شود، تأییدیه‌ای برای (N+1)-هستار فراهم می‌کند که منبع داده‌ها همان است که هستار همتای (N+1)-لایه ادعا کرده است.

---

1 - Practical realizations
2 - Liveness check
3 - Data origin authentication

خدمت احراز هویت مبدأ داده‌ها، تأییدیه‌ای برای منبع یک واحد داده‌ای فراهم می‌کند. این خدمت، محافظتی در برابر دوتایی‌شدن[1] یا تغییر واحدهای داده‌ای فراهم نمی‌کند.

۵-۲-۲ کنترل دسترسی

این خدمت برای منابع دسترس‌پذیر از طریق OSI، محافظت در برابر استفاده‌های غیرمجاز را فراهم می‌کند. این منابع ممکن است منابع OSI یا غیر OSI باشند که از طریق پروتکل‌های OSI مورد دسترسی قرار می‌گیرند. این خدمت محافظتی می‌تواند بر روی انواع مختلف دسترسی به منبع (به‌عنوان مثال، استفاده از منابع ارتباطی، خواندن، نوشتن، یا حذف یک منبع اطلاعاتی، اجرای منابع پردازشی) یا به همه دسترسی‌ها به یک منبع به‌کارگرفته شود.

کنترل دسترسی منطبق با خط مشی‌های امنیتی مختلف خواهد بود. (به زیربند ۶-۲-۱-۱ مراجعه شود.)

۵-۲-۳ محرمانگی داده‌ها

این خدمات برای محافظت از داده‌ها در برابر افشای غیرمجاز به‌صورتی که در زیر توضیح داده می‌شود، ارائه می‌شوند.

۵-۲-۳-۱ محرمانگی اتصال[2]

این خدمت، محرمانگی را برای همه (N)-داده‌های کاربر در یک (N)-اتصال فراهم می‌کند.

یادآوری- بسته به استفاده و لایه، ممکن است این خدمت برای محافظت از همه داده‌ها مناسب نباشد، برای مثال داده‌های پیشتاز[3] یا داده‌های موجود در یک درخواست اتصال.

۵-۲-۳-۲ محرمانگی بی‌اتصال[4]

این خدمت محرمانگی را برای همه (N)-داده‌های کاربر در یک SDU-(N) بی‌اتصال منفرد فراهم می‌کند.

۵-۲-۳-۳ محرمانگی فیلد انتخابی[5]

این خدمت محرمانگی را برای فیلدهای انتخاب‌شده‌ی درون (N)-داده‌های کاربر در یک (N)-اتصال یا یک SDU-(N) بی‌اتصال منفرد فراهم می‌کند.

۵-۲-۳-۴ محرمانگی جریان ترافیک[6]

این خدمت محافظت از اطلاعاتی را فراهم می‌کند که ممکن است از مشاهده جریان‌های ترافیک به‌دست آیند.

---

1 - Duplication
2 - Connection
3 - Expedited
4 - Connectionless confidentiality
5 - Selective field confidentiality
6 - Traffic flow confidentiality

۵-۲-۴ یکپارچگی داده‌ها

این خدمات با تهدیدات فعال مقابله کرده و ممکن است به یکی از روش‌های مطرح شده در زیربندهای زیر باشد.

یادآوری- استفاده از خدمت احراز هویت هستار همتا در شروع اتصال و خدمت یکپارچگی داده در طول عمر اتصال می‌تواند تأییدیه‌ای را برای همه واحدهای داده‌ای که در اتصال منتقل می‌شوند و یکپارچگی آن واحدهای داده‌ای فراهم کند. به‌علاوه، ممکن است که تشخیص تکرار واحدهای داده‌ای را برای مثال با استفاده از شماره‌های دنباله[1] فراهم کند.

۵-۲-۴-۱ یکپارچگی اتصال با بازیابی[2]

این خدمت یکپارچگی همه (N)-داده‌های کاربر را در یک (N)-اتصال فراهم کرده و هرگونه تغییر، درج، حذف و بازپخش هر داده‌ای را در کل دنباله SDU (به همراه تلاش برای بازیابی آن) تشخیص می‌دهد.

۵-۲-۴-۲ یکپارچگی اتصال بدون بازیابی[3]

مطابق زیربند ۵-۲-۴-۱، اما بدون تلاش برای بازیابی.

۵-۲-۴-۳ یکپارچگی فیلد انتخابی اتصال

این خدمت یکپارچگی فیلدهای انتخابی درون (N)-داده‌های کاربر مربوط به یک SDU (N)-لایه را فراهم می‌کند که بر روی یک اتصال منتقل می‌شوند و از روشی برای تشخیص تغییر، درج یا بازپخش فیلدهای انتخابی استفاده می‌کند.

۵-۲-۴-۴ یکپارچگی بی‌اتصال[4]

این خدمت هنگامی که به وسیله (N)-لایه فراهم شود، تضمین یکپارچگی برای هستار درخواست‌کننده (N+1)-لایه فراهم می‌کند.

این خدمت یکپارچگی SDU بی‌اتصال منفرد را فراهم کرده و ممکن است به این صورت باشد که تعیین کند که آیا یک SDU دریافت‌شده، تغییر کرده است یا خیر. علاوه بر این، یک نوع محدود از تشخیص بازپخش نیز ممکن است فراهم شده باشد.

۵-۲-۴-۵ یکپارچگی بی‌اتصال فیلد انتخابی[5]

این خدمت یکپارچگی فیلدهای منتخب درون یک SDU بی‌اتصال منفرد را فراهم کرده و به این صورت که تعیین کند که آیا آن فیلدهای منتخب تغییر یافته‌اند یا خیر، عمل می‌کند.

۵-۲-۵ انکارناپذیری[6]

این خدمت می‌تواند به‌صورت یک یا هر دو صورت زیر باشد.

---

1 - Sequence number
2 - Connection integrity with recovery
3 - Connection integrity without recovery
4 -Connectionless integrity
5 - Selective field connectionless integrity
6 - Non-repudiation

۵-۲-۵-۱ انکارناپذیری به همراه اثبات مبدأ[1]

مدرکی دال بر اثبات مبدأ داده‌ها برای دریافت‌کننده‌ی داده‌ها فراهم می‌شود. این کار باعث محافظت در برابر هر تلاشی به‌وسیله فرستنده از اینکه به اشتباه از ارسال داده‌ها یا محتوای آن‌ها امتناع کند، می‌شود.

۵-۲-۵-۲ انکارناپذیری به همراه اثبات تحویل[2]

مدرکی دال بر اثبات تحویل داده‌ها در اختیار فرستنده داده‌ها قرار می‌گیرد. این کار باعث محافظت در برابر هر تلاشی به‌وسیله گیرنده از اینکه به اشتباه از دریافت داده‌ها یا محتوای آن‌ها امتناع کند، می‌شود.

۵-۳ سازوکارهای امنیتی خاص[3]

سازوکارهایی که در ادامه توضیح داده خواهند شد ممکن است با (N)-لایه مناسبی برای فراهم‌سازی خدماتی که در زیربند ۵-۲ توضیح داده شد، همکاری داشته باشند.

۵-۳-۱ رمزگذاری

۵-۳-۱-۱ رمزگذاری می‌تواند محرمانگی داده‌ها یا اطلاعات جریان ترافیک را فراهم ساخته و می‌تواند به‌عنوان جزیی برای تکمیل تعدادی از سازوکارهای امنیتی دیگر که در بخش‌های بعدی توضیح داده می‌شوند، عمل کند.

۵-۳-۱-۲ الگوریتم‌های رمزگذاری ممکن است برگشت‌پذیر یا برگشت‌ناپذیر باشند. دو دسته‌بندی کلی برای الگوریتم‌های برگشت‌پذیر وجود دارد:

الف- رمزگذاری متقارن (یا کلید سری[4]) که در آن آگاهی از کلید رمزگذاری به مثابه آگاهی از کلید رمزگشایی بوده و بالعکس؛ و

ب- رمزگذاری نامتقارن (یا کلید عمومی) که در آن آگاهی از کلید رمزگذاری به مثابه آگاهی از کلید رمزگشایی نبوده و بالعکس. این دو کلید در چنین سامانه‌ای اغلب تحت عنوان «کلید عمومی» و «کلید خصوصی» نامیده می‌شوند.

الگوریتم‌های رمزگذاری برگشت‌ناپذیر ممکن است از یک کلید استفاده کنند یا نکنند. هنگامی که از یک کلید استفاده می‌شود آن کلید ممکن است عمومی یا سرّی باشد.

۵-۳-۱-۳ وجود یک سازوکار رمزگذاری به معنی آن است که از سازوکار مدیریت کلید نیز استفاده می‌شود، مگر در مورد برخی الگوریتم‌های رمزگذاری برگشت‌ناپذیر. برخی از راهنماها در مورد روش‌های مدیریت کلید در زیربند ۸-۱ آورده شده است.

۵-۳-۲ سازوکارهای امضای دیجیتالی[5]

این سازوکارها دو رویه را تعریف می‌کنند:

---

1 - Proof of origin
2 - Proof of delivery
3 - Specific security mechanisms
4 - Secret key
5 - Digital signature mechanisms

الف- امضای یک واحد داده‌ای؛ و
ب- درستی‌سنجی[1] یک واحد داده‌ای امضاشده.
فرآیند نخست از اطلاعاتی استفاده می‌کند که برای امضاکننده خصوصی (یعنی یکتا و محرمانه) است. فرآیند دوم از رویه‌ها و اطلاعاتی استفاده می‌کند که در دسترس عموم قرار داشته، اما نمی‌توان از آن اطلاعات خصوصی امضاکننده را استنتاج کرد.

۵-۳-۲-۱ فرآیند امضا دربرگیرنده یا رمزگذاری یک واحد داده‌ای یا تولید یک مقدار وارسی رمزنگاشتی برای واحد داده‌ای، با استفاده از اطلاعات خصوصی امضاکننده به‌عنوان یک کلید خصوصی است.

۵-۳-۲-۲ فرآیند درستی‌سنجی امضا دربرگیرنده رویه‌ها و اطلاعات عمومی برای تعیین این است که آیا امضا همان است که به‌وسیله اطلاعات خصوصی امضاکننده تولید شده بود یا خیر.

۵-۳-۲-۳ ویژگی اساسی سازوکار امضا آن است که امضا تنها می‌تواند به‌وسیله اطلاعات خصوصی امضاکننده تولید شده باشد. بنابراین وقتی که امضا درستی‌سنجی شد، سپس می‌تواند برای یک طرف سوم (مانند یک قاضی یا داور) اثبات شود، در هر زمانی که فقط یگانه دارنده‌ی اطلاعات خصوصی توانسته است امضا را تولید کرده باشد.

۵-۳-۳ سازوکارهای کنترل دسترسی[2]

۵-۳-۳-۱ این سازوکارها ممکن است از هویت احرازشده یک هستار یا اطلاعات درباره آن هستار (نظیر عضویت در یک مجموعه معلوم از هستارها) یا قابلیت‌های آن هستار استفاده نموده تا حقوق دسترسی به آن را تعیین و استفاده کند. اگر آن هستار در تلاش باشد که به یک منبع غیرمجاز یا به یک منبع مجاز با نوع نادرستی از دسترسی، دسترسی داشته باشد، آنگاه کارکرد کنترل دسترسی انجام آن تلاش را رد[3] کرده و به‌علاوه ممکن است منجر به گزارش‌کردن رویداد[4] برای مقاصد تولید هشدار[5] و/یا ثبت در بخشی از دنباله‌ی ممیزی امنیت شود. هر نوع اخطار به فرستنده یک دسترسی منع‌شده برای انتقال داده‌های بی‌اتصال می‌تواند فقط به‌عنوان نتیجه اجرای کنترل‌های دسترسی در مبدأ فراهم شده باشد.

۵-۳-۳-۲ سازوکارهای کنترل دسترسی ممکن است، برای مثال، بر مبنای استفاده از یک یا چند مورد از موارد زیر باشند:
الف- پایگاه‌های اطلاعاتی کنترل دسترسی، جایی که حقوق دسترسی هستارهای همتا نگهداری می‌شود. این اطلاعات ممکن است به‌وسیله مراکز مجازشناسی[6] یا به‌وسیله هستار مورد دسترسی نگهداری شوند و ممکن است به‌صورت یک ساختار سلسله‌مراتبی یا توزیع‌شده از فهرست یا ماتریسی از کنترل دسترسی باشند. از قبل فرض می‌شود که احراز هویت هستار همتا تضمین شده است؛

1 - Verifying
2 - Access control mechanisms
3 - Reject
4 - Incident
5 - Alarm
6 - Authorization

ب- اطلاعات احراز هویت، مانند کلمه‌های عبور، مالکیت و ارائه متعاقب آن، مدرکی دال بر مجازشناسی هستار دسترسی یابنده است؛
پ- قابلیت‌ها، مالکیت و ارائه بعدی آن‌ها، مدرکی دال بر حق دسترسی هستار یا منبع تعریف‌شده به وسیله قابلیت است؛

یادآوری- یک قابلیت باید غیر قابل جعل بوده و باید به روشی قابل اعتماد حمل شود.

ت- برچسب‌های امنیتی، درصورت مرتبط شدن به یک هستار، ممکن است برای اعطاء یا منع دسترسی، به‌طور کلی طبق خط مشی‌های امنیتی، مورد استفاده قرار گیرند؛
ث- زمان تلاش برای دسترسی؛
ج- مسیر تلاش برای دسترسی؛ و
چ- مدت دسترسی.

۵-۳-۳-۳ سازوکارهای کنترل دسترسی می‌توانند یا در پایان همبستگی ارتباطات[1] و/یا هر نقطه میانی آن به‌کارگرفته شوند.
کنترل‌های دسترسی که در مبدأ یا هر نقطه‌ی میانی به به‌کارگرفته می‌شوند برای تعیین اینکه آیا فرستنده برای ارتباط با گیرنده مجاز بوده یا خیر و/یا برای استفاده از منابع مورد استفاده قرار می‌گیرند.
نیازمندی‌های سازوکارهای کنترل دسترسی در سطح همتا در نقطه‌ی مقصد یک انتقال داده‌های بی‌اتصال باید از پیش به‌وسیله مبدأ شناخته شده باشند و علاوه بر این باید در پایگاه اطلاعاتی مدیریت امنیت ثبت شده باشند. (به زیربندهای ۶-۲ و ۸-۱ مراجعه شود.)

۵-۳-۴ سازوکارهای یکپارچگی داده[2]

۵-۳-۴-۱ دو جنبه‌ی یکپارچگی داده عبارتند از: یکپارچگی یک واحد یا فیلد داده‌ای منفرد و یکپارچگی جریانی از واحدها یا فیلدهای داده‌ای. به‌طور کلی، از سازوکارهای مختلفی برای فراهم‌سازی این دو نوع خدمت یکپارچگی استفاده می‌شود، با وجودی که فراهم‌سازی مورد دوم بدون مورد نخست عملی نیست.

۵-۳-۴-۲ تعیین یکپارچگی یک واحد داده‌ای منفرد شامل دو فرآیند است، یکی در هستار فرستنده و دیگری در هستار گیرنده. هستار فرستنده مقداری را به انتهای واحد داده‌ای اضافه می‌کند که این مقدار تابعی از خود داده‌ها است. این مقدار ممکن است یک اطلاعات مکمل مانند یک کد وارسی بستک[3] و/یا مقدار وارسی رمزنگاشتی باشد و ممکن است که خودش رمزشده باشد. هستار گیرنده یک مقدار معادل را تولید و آن را با مقدار دریافت‌شده مقایسه نموده تا تعیین کند که آیا داده‌ها در مسیر انتقال تغییر یافته‌اند یا خیر. این سازوکار به تنهایی قادر نیست که در برابر بازپخش یک واحد داده‌ای منفرد محافظت به عمل آورد. در

1 - Communications association
2 - Data integrity mechanisms
3 - Block check code

لایه‌های مناسبی از معماری، تشخیص فرابری ممکن است منجر به یک عمل بازیابی (برای مثال از طریق بازپخش یا تصحیح خطا) در آن لایه یا لایه‌های بالاتر شود.

۵-۳-۴-۳ برای انتقال داده‌های حالت اتصال، محافظت از یکپارچگی دنباله‌ای از واحدهای داده‌ای (مانند محافظت در برابر به‌هم‌زدن ترتیب، از دست دادن، بازپخش و درج یا تغییر داده‌ها) نیازمند برخی از انواع اضافی ترتیب‌دهی[1] صریح، مانند شماره‌گذاری دنباله[2]، مهرزنی زمانی[3]، یا زنجیره‌سازی رمزنگاشتی[4] است.

۵-۳-۴-۴ برای انتقال داده‌های بی‌اتصال، مهرزنی زمانی ممکن است برای فراهم‌سازی شکل محدودی از محافظت در برابر بازپخش واحدهای داده مجزا استفاده شود.

۵-۳-۵ سازوکار تبادل احراز هویت[5]

۵-۳-۵-۱ برخی از روش‌هایی که ممکن است برای تبادل احراز هویت استفاده شوند عبارتند از:

الف- استفاده از اطلاعات احراز هویت، مانند کلمه‌های عبور فراهم‌شده به‌وسیله یک هستار فرستنده و بررسی شده به‌وسیله یک هستار گیرنده؛

ب- فنون رمزنگاری؛ و

پ- استفاده از ویژگی‌ها و/یا دارایی‌های هستار.

۵-۳-۵-۲ سازوکارها ممکن است در (N)-لایه به‌منظور انجام احراز هویت هستار همتا به‌کار گرفته شوند. اگر سازوکار موفق به انجام احراز هویت هستار نشود، این کار باعث رد یا ختم اتصال شده و همچنین ممکن است باعث افزودن یک درایه[6] در دنباله ممیزی امنیت و/یا یک گزارش به یک مرکز مدیریت امنیت شود.

۵-۳-۵-۳ هنگامی که از فنون تبادل احراز هویت استفاده می‌شود، ممکن است با پروتکل‌های «دست‌دهی»[7] برای محافظت در برابر بازپخش (نظیر، تضمین زنده‌بودن) ترکیب شوند.

۵-۳-۵-۴ انتخاب‌های فنون تبادل احراز هویت به عواقب آن‌ها بستگی دارد. در بسیاری از موارد نیاز است این فنون به همراه موارد زیر استفاده شوند:

الف- مهرزنی زمانی و ساعت‌های همگام‌شده[8]؛

ب- دست‌دهی دو و سه سویه (به‌ترتیب، برای احراز هویت یک‌طرفه و دوطرفه)؛ و

پ- خدمات انکارناپذیری که به‌وسیله سازوکارهای امضای دیجیتالی و/یا گواهی رسمی حاصل می‌شوند.

---

1 - Ordering
2 - Sequence numbering
3 - Time stamping
4 - Cryptographic chaining
5 - Authentication exchange mechanism
6 - Entry
7 - Handshaking
8 - Synchronized clocks

۵-۳-۶ سازوکارهای لت‌گذاری ترافیک[1]

سازوکارهای لت‌گذاری ترافیک را می‌توان برای فراهم‌سازی سطوح مختلف محافظت در برابر تحلیل ترافیک مورد استفاده قرار داد. این سازوکار تنها زمانی مؤثر است که لت‌گذاری ترافیک به‌وسیله یک خدمت محرمانگی محافظت شود.

۵-۳-۷ سازوکارهای کنترل مسیریابی[2]

۵-۳-۷-۱ مسیرها را می‌توان یا به‌صورت پویا یا از پیش تعیین‌شده انتخاب کرد، طوری‌که تنها از زیرشبکه‌ها، رله‌ها یا پیوندهای به‌طور فیزیکی امن استفاده کرد.

۵-۳-۷-۲ سامانه‌های پایانی در هنگام تشخیص حملات فرابری ماندگار[3]، می‌خواهند که به فراهم‌کننده خدمت شبکه دستور دهند که یک اتصال از طریق یک مسیر متفاوت ایجاد کند.

۵-۳-۷-۳ داده‌هایی که برچسب‌های خاص امنیتی را حمل می‌کنند، ممکن است به‌وسیله خط‌مشی امنیتی از عبور از زیرشبکه‌ها، رله‌ها یا پیوندهای خاصی منع شده باشند. همچنین آغازگر یک اتصال (یا فرستنده یک واحد داده‌ای بی‌اتصال) ممکن است پیش‌بینی‌های احتیاطی مسیریابی را تعیین کرده باشد که نیازمند منع‌کردن آن زیرشبکه‌ها، پیوندها یا رله‌های خاص باشد.

۵-۳-۸ سازوکار گواهی رسمی[4]

خصوصیت‌هایی درباره داده‌های مبادله‌شده بین دو هستار یا بیشتر، نظیر یکپارچگی، مبدأ، زمان و مقصد را می‌توان با استفاده از یک سازوکار گواهی رسمی تضمین کرد. این تضمین به وسیله یک دفتر اسناد رسمی[5] ثالث که مورد اعتماد هستارهای ارتباطی است فراهم می‌شود که اطلاعات مورد نیاز برای فراهم‌سازی تضمین مورد درخواست را به روشی قابل اعتماد نگهداری می‌کند. هر نمونه از ارتباطات ممکن است از امضای رقمی، رمزگذاری و سازوکارهای یکپارچگی استفاده کند که مناسب خدمات ارایه‌شده به‌وسیله دفتر اسناد رسمی است. هنگامی که چنین سازوکار گواهی رسمی فراخوانی می‌شود، داده‌ها از طریق نمونه‌های محافظت‌شده ارتباطات مابین هستارهای ارتباطی مبادله می‌شوند.

۵-۴ سازوکارهای امنیتی فراگیر[6]

در این زیربند، تعدادی از سازوکارها توضیح داده می‌شوند که اختصاص به هیچ خدمت خاصی ندارند. بنابراین در بند ۷ این سازوکارها طوری توضیح داده می‌شوند که به‌طور صریح مربوط به لایه خاصی نباشند. برخی از این سازوکارها را می‌توان جنبه‌هایی از مدیریت امنیت دانست. (به بند ۸ مراجعه شود.) به‌طور کلی، اهمیت این سازوکارها به‌طور مستقیم به سطح امنیت مورد نیاز مرتبط است.

---

1 - Traffic padding
2 - Routing control mechanism
3 - Persistent manipulation attacks
4 - Notarization
5 - Notary
6 - Pervasive security mechanisms

۵-۴-۱ کارکرد قابل اعتماد

۵-۴-۱-۱ کارکرد قابل اعتماد باید برای بسط حوزه، یا برقراری اثر سایر سازوکارهای امنیتی مورد استفاده قرار گیرد. هر کارکردی که به‌طور مستقیم (یا غیرمستقیم) دسترسی به سازوکارهای امنیتی را فراهم می‌کند، باید قابل اعتماد[1] باشد.

۵-۴-۱-۲ رویه‌هایی که برای تضمین اعتماد ممکن است در سخت‌افزار یا نرم‌افزار قرار داده شوند خارج از حوزه این استاندارد هستند و در هر حالت با توجه به سطوح تهدید ملاحظه‌شده و ارزش اطلاعاتی که باید محافظت شوند، فرق می‌کنند.

۵-۴-۱-۳ این رویه‌ها به‌طور کلی بسیار پرهزینه بوده و پیاده‌سازی آن‌ها دشوار است. این مشکلات را می‌توان با انتخاب یک معماری که اجازه پیاده‌سازی کارکردهای امنیتی در پیمانه‌هایی که می‌توانند جدا از، و فراهم‌شده از، کارکردهای غیرامنیتی مرتبط ایجاد شوند را می‌دهند، کمینه کرد.

۵-۴-۱-۴ هر گونه محافظت از ارتباطات بالای لایه‌ای که محافظت در آن به‌کارگیری شده است باید با ابزارهای دیگر، مانند کارکرد قابل اعتماد مناسب، فراهم شود.

۵-۴-۲ برچسب‌های امنیتی[2]

منابع دربرگیرنده اقلام داده‌ای[3] ممکن است دارای برچسب‌های امنیتی باشند که به‌عنوان مثال سطح حساسیت آن‌ها را تعیین کند. اغلب ضروری است که برچسب‌های امنیتی به همراه داده‌های در حال انتقال حمل شوند. یک برچسب امنیتی ممکن است داده‌های اضافی مرتبط به داده‌های منتقل شده باشد یا آنکه ممکن است ضمنی باشد، برای مثال، مورد اشاره به‌وسیله استفاده از یک کلید خاص برای رمزگذاری داده‌ها یا مورد اشاره به‌وسیله زمینه[4] داده‌ها، نظیر منبع یا مسیر آن. به علاوه، برچسب‌های امنیتی باید به‌طور امن به داده‌هایی که به آن‌ها مرتبط شده‌اند، وابسته‌سازی شوند.

۵-۴-۳ تشخیص رویداد[5]

۵-۴-۳-۱ تشخیص رویدادهای مرتبط با امنیت شامل تشخیص نقض‌های[6] آشکار از امنیت بوده و همچنین ممکن است شامل تشخیص رویدادهای «عادی»، نظیر دسترسی موفقیت‌آمیز (یا ورود به سامانه[7]) باشد. رویدادهای مرتبط با امنیت ممکن است به‌وسیله هستارهای درون OSI که دربرگیرنده سازوکارهای امنیتی هستند، تشخیص داده شوند. مشخصات آنچه که یک رویداد را تشکیل می‌دهد به‌وسیله مدیریت سامان‌دهی

1 - Trustworthy
2 - Security Labels
3 - Data items
4 - Context
5 - Event Detection
6 - Violations
7 - Logon

رویداد[1] نگهداری می‌شود. (به زیربند ۸-۳-۱ مراجعه شود.) تشخیص رویدادهای مختلف مرتبط با امنیت ممکن است به‌عنوان مثال منجر به یک یا چند مورد از عمل‌های زیر شوند:

الف- گزارش‌دادن محلی رویداد؛

ب- گزارش‌دادن از راه دور رویداد ؛

پ- ثبت سابقه رویداد (به زیربند ۵-۴-۳ مراجعه شود.) و

ت- عمل بازیابی (به زیربند ۵-۴-۴ مراجعه شود.)

مثال‌هایی از چنین رویدادهای مرتبط با امنیت عبارتند از:

الف- یک نقض امنیت خاص؛

ب- یک رویداد منتخب خاص؛ و

پ- یک سرریز شماره تعداد وقایع.

۵-۴-۳-۲ تدوین استاندارد در این حوزه، ارسال[2] اطلاعات مرتبط برای گزارش و ثبت سابقه رویداد و تعریف نحوی و معنایی مورد استفاده برای ارسال گزارش رویداد و ثبت سابقه رویداد را مدنظر قرار خواهد داد.

۵-۴-۴ دنباله ممیزی امنیت

۵-۴-۴-۱ دنباله‌های ممیزی امنیت یک سازوکار امنیتی با ارزش را فراهم می‌کند، به نحوی که به‌طور بالقوه اجازه می‌دهند که تشخیص و بررسی رخنه‌های امنیتی به‌وسیله یک ممیزی امنیت بعدی امکان‌پذیر باشد. ممیزی امنیت یک بازبینی و آزمون مستقل رکوردها و فعالیت‌های سامانه به‌منظور آزمون کفایت کنترل‌های سامانه، برای اطمینان از مطابقت با خط‌مشی‌ها و رویه‌های عملیاتی، برای کمک به ارزیابی میزان خسارت و توصیه هرگونه تغییرات لازم در کنترل‌ها، خط‌مشی و رویه‌ها است. یک ممیزی امنیت نیازمند ثبت اطلاعات مرتبط با امنیت در یک دنباله ممیزی امنیت و تحلیل و گزارش اطلاعات دنباله ممیزی امنیت است. ثبت و ضبط سابقه به‌عنوان یک سازوکار امنیتی در نظرگرفته شده و در این بخش توضیح داده می‌شود. تحلیل و تولید گزارش یک کارکرد مدیریت امنیت محسوب می‌شود. (به زیربند ۸-۳-۲ مراجعه شود.)

۵-۴-۴-۲ جمع‌آوری اطلاعات دنباله ممیزی امنیت ممکن است منطبق با نیازمندی‌های مختلف به وسیله تعیین انواع رویدادهای مرتبط با امنیت که باید ثبت شوند انجام شود. (برای مثال، نقض‌های امنیتی آشکار یا تکمیل عملیات موفقیت‌آمیز)

وجود آگاهانه دنباله ممیزی امنیت ممکن است به‌عنوان یک عامل بازدارنده برای برخی از منابع بالقوه حملات امنیتی به‌کار رود.

1 - Event Handling Management
2 - Transmission

۵-۴-۴-۳ ملاحظات دنباله ممیزی امنیت OSI اطلاعاتی که باید به‌طور انتخابی ثبت شوند، اینکه تحت چه شرایطی باید این اطلاعات ثبت شوند و تعریف نحوی و معنایی که باید برای تبادل اطلاعات دنباله ممیزی امنیت مورد استفاده قرار گیرند را مشخص می‌کند.

۵-۴-۵ بازیابی امنیت

۵-۴-۵-۱ بازیابی امنیت با درخواست‌ها از سازوکارهایی همچون کارکردهای مدیریت و سامان‌دهی رویداد سروکار دارد و عمل‌های بازیابی را به‌عنوان نتیجه به‌کارگیری مجموعه‌ای از قواعد انجام می‌دهد. این عمل‌های بازیابی ممکن است به سه صورت زیر باشند.

الف- فوری؛

ب- موقتی؛ و

پ- طولانی مدت.

برای مثال:

عمل‌های فوری ممکن است یک رد فوری عملیات، نظیر قطع اتصال را ایجاد کنند.

عمل‌های موقتی ممکن است بی‌اعتبار شدن موقتی یک هستار را ایجاد کنند.

عمل‌های طولانی مدت ممکن است معرفی یک هستار در «فهرست سیاه»[1] یا تغییر یک کلید را ایجاد کنند.

۵-۴-۵-۲ موضوعات استانداردسازی شامل پروتکل‌هایی برای عمل‌های بازیابی و برای مدیریت بازیابی امنیت است (به زیربند ۸-۳-۳ مراجعه شود.)

۵-۵ شرح روابط بین خدمات و سازوکارهای امنیتی

جدول ۱ شرح می‌دهد که کدام سازوکارها، به تنهایی یا در ترکیب با سازوکارهای دیگر، برای فراهم‌سازی هر خدمت مناسب به نظر می‌رسد. این جدول نگاهی اجمالی بر این روابط داشته و قطعی نیست.

خدمات و سازوکارهای اشاره شده در جدول ۱ در زیربندهای ۵-۲ و ۵-۳ توضیح داده شده‌اند. همچنین، روابط به‌طور کامل در بخش ۶ توضیح داده شده‌اند.

1 - Black List

جدول ۱- روابط بین خدمات و سازوکارهای امنیتی

سازوکار / خدمت	رمزگذاری	امضای دیجیتالی	کنترل دسترسی	یکپارچگی داده	تبادل احراز هویت	لت‌گذاری ترافیک	کنترل مسیریابی	گواهی رسمی
احراز هویت هستار همتا	بله	بله	•	•	بله	•	•	•
احراز هویت مبدأ داده‌ها	بله	بله	•	•	•	•	•	•
خدمت کنترل دسترسی	•	•	بله	•	•	•	•	•
محرمانگی اتصال	بله	•	•	•	•	•	بله	•
محرمانگی بدون‌اتصال	بله	•	•	•	•	•	بله	•
محرمانگی فیلد انتخابی	بله	•	•	•	•	•	•	•
محرمانگی جریان ترافیک	بله	•	•	•	•	بله	بله	•
یکپارچگی اتصال با بازیابی	بله	•	•	بله	•	•	•	•
یکپارچگی اتصال بدون بازیابی	بله	•	•	بله	•	•	•	•
یکپارچگی اتصال فیلد انتخابی	بله	•	•	بله	•	•	•	•
یکپارچگی بی‌اتصال	بله	بله	•	بله	•	•	•	•
یکپارچگی بی‌اتصال فیلد انتخابی	بله	بله	•	بله	•	•	•	•
انکارناپذیری، مبدأ	•	بله	•	بله	•	•	•	بله
انکارناپذیری، تحویل	•	بله	•	بله	•	•	•	بله

کوته‌نوشت‌ها:
بله: این سازوکار به تنهایی و یا در ترکیب با سازوکارها مناسب محسوب می‌شود.
• مکانیزم متاسب محسوب نمی‌شود.

۶ روابط بین خدمات، سازوکارها و لایه‌ها

۶-۱اصول لایه‌بندی امنیت

۶-۱-۱ اصول زیر به‌منظور تعیین نحوه اختصاص خدمات امنیتی به لایه‌ها و در نتیجه جای‌گذاری سازوکارهای امنیتی در لایه‌ها استفاده شده‌اند:

الف- تعداد راه‌های جایگزین برای حصول به یک خدمت باید کمینه شود؛
ب- قابل قبول است که به‌وسیله فراهم‌سازی خدمات امنیتی در بیش از یک لایه، سامانه‌های امنیتی ساخته شوند؛
پ- کارکرد اضافی مورد نیاز برای امنیت نباید به‌طور غیرضروری کارکردهای موجود OSI را تکرار کند؛
ت- از نقض استقلال لایه‌ای باید جلوگیری شود؛
ث- میزان کارکرد قابل اعتماد باید کمینه شود؛
ج- هرجا یک هستار وابسته به یک سازوکار امنیتی فراهم شده به‌وسیله یک هستار در لایه‌ای پایین‌تر باشد، هر لایه میانی باید طوری ساخته شود که نقض امنیتی غیرعملی[1] باشد؛
چ- هرجا که امکان‌پذیر باشد، کارکردهای امنیتی اضافی یک لایه باید طوری تعریف شوند که از پیاده‌سازی آن‌ها به‌صورت پیمانه(های) خودشمول[2] ممانعت نشود؛ و
ح- فرض می‌شود که این استاندارد برای سامانه‌های باز متشکل از سامانه‌های پایانی حاوی همه هفت لایه شبکه و سامانه‌های رله به کارگیری می‌شود.

۶-۱-۲ تعاریف خدمت در هر لایه ممکن است نیازمند تغییر برای فراهم‌سازی درخواست‌های خدمات امنیتی در همان لایه یا در لایه زیرین باشد.

۶-۲ مدل فراخوانی، مدیریت و استفاده از (N)-خدمات محافظت‌شده

این بند فرعی باید به همراه بند ۸ مطالعه شود که شامل یک بحث کلی درباره مسائل مدیریت امنیت است. قصد آن است که خدمات و سازوکارهای امنیتی بتوانند به‌وسیله هستار مدیریت از طریق واسط مدیریت و/یا به وسیله فراخوانی خدمت فعال شوند.

۶-۲-۱ تعیین ویژگی‌های محافظتی برای نمونه‌ای از ارتباط

۶-۲-۱-۱ کلیات

این زیربند فراخوانی مربوط به محافظت از نمونه‌های اتصال‌گرا و بی‌اتصال ارتباط را توضیح می‌دهد. برای ارتباط‌های اتصال‌گرا، خدمات محافظتی به‌طور معمول در زمان برقراری اتصال درخواست/اعطاء می‌شوند. در مورد فراخوانی خدمت بی‌اتصال، محافظت برای هر نمونه از یک درخواست UNITDATA، درخواست/اعطاء می‌شود.
به‌منظور ساده‌سازی توضیحات زیر، از اصطلاح «درخواست خدمت» به معنی برقراری یک اتصال یا یک درخواست UNITDATA استفاده می‌شود. فراخوانی محافظت از داده‌های منتخب با درخواست محافظت فیلد انتخابی قابل حصول است. برای مثال، این کار را می‌توان با برقراری چندین اتصال انجام داد که هر کدام دارای نوع یا سطح متفاوتی از محافظت است.

1 - Impractical
2 - Self-contained

این معماری امنیتی با خط‌مشی‌های امنیتی متنوع که شامل انواع مبتنی بر قاعده، مبتنی بر هویت و ترکیبی از هر دو است، سازگاری دارد. این معماری امنیتی با محافظتی که به‌صورت مدیریتی به‌کارگیری‌شده[1]، به‌طور پویا انتخاب می‌شود و ترکیبی از هر دو است، نیز سازگار است.

۶-۲-۱-۲ درخواست‌های خدمت

برای هر درخواست (N)-خدمت، (N+1)-هستار ممکن است یک محافظت مورد نظر دلخواه را درخواست کرده باشد. درخواست (N)-خدمت، خدمات امنیتی به همراه پارامترها و هر نوع اطلاعات اضافی مرتبط (مانند اطلاعات حساسیت و/یا برچسب‌های امنیتی) را برای حصول محافظت امنیتی مورد نظر مشخص می‌کند.

قبل از هر نمونه از ارتباط، (N)-لایه مجبور به دسترسی به پایگاه اطلاعات مدیریت امنیت (SMIB) است. (به زیربند ۸-۱ مراجعه شود.) هر SMIB حاوی اطلاعات نیازهای محافظتی است که به‌صورت مدیریتی به‌کارگیری‌شده و مرتبط با (N+1)-هستار است. کارکرد قابل اعتماد برای تحقق این نیازمندی‌های امنیتی به‌کارگیری‌شده به‌طور مدیریتی، مورد نیاز است.

فراهم‌سازی ویژگی‌های امنیتی برای یک نمونه ارتباط اتصال‌گرا ممکن است نیازمند مذاکره‌ی خدمات امنیتی مورد نیاز با همدیگر باشد. رویه‌هایی را که برای سازوکارها و پارامترهای مذاکره لازم است می‌توان یا به‌صورت یک رویه مجزا یا به‌صورت یک بخش کامل از یک رویه برقراری اتصال اجرا کرد.

زمانی که مذاکره به‌صورت یک رویه مجزا اجرا می‌شود، نتایج موافقت (یعنی، بسته به نوع سازوکارهای امنیتی و پارامترهای امنیتی که برای فراهم‌سازی چنین خدمات امنیتی مورد نیاز هستند.) به پایگاه اطلاعاتی مدیریت امنیت وارد می‌شوند. (به زیربند ۸-۱ مراجعه شود.)

وقتی که مذاکره به‌صورت یک بخش کامل از یک رویه برقراری اتصال عادی اجرا می‌شود، نتایج قواعد بین (N)-هستارها، به‌طور موقتی در SMIB ذخیره خواهد شد. قبل از مذاکره هر (N)-هستار به اطلاعات مورد نیاز برای مذاکره به SIMB دسترسی خواهد داشت.

اگر درخواست خدمت، نیازهای به‌کارگیری‌شده به‌طور مدیریتی که در SMIB برای (N+1)-هستار ثبت شده‌اند را نقض کند، توسط (N)-لایه رد خواهد شد.

(N)-لایه همچنین به خدمات محافظتی درخواست‌شده، هر خدمت امنیتی تعریف‌شده در SMIB به‌صورت اجباری را برای به‌دست آوردن محافظت امنیتی مورد نظر اضافه می‌کند.

اگر (N+1)-هستار هیچ نوع محافظت امنیتی مورد نظر را مشخص نکند، (N)-لایه از یک خط‌مشی امنیتی سازگار با SMIB پیروی خواهد کرد. این کار به‌منظور پیشبرد ارتباط با استفاده از یک محافظت امنیتی پیش‌فرض در محدوده تعریف‌شده برای (N+1)-هستار درSMIB، خواهد بود.

1 - Administratively imposed

۶-۲-۲ فراهم‌سازی خدمات محافظتی

پس از ترکیب نیازهای امنیتی که به‌طور مدیریتی به‌کارگیری‌شده و به‌طور پویا تعیین شده‌اند، همان‌گونه که در زیربند ۶-۲-۱ توضیح داده شد، (N)-لایه تلاش خواهد کرد که حداقل محافظت مورد نظر حاصل شود. این کار یا از طریق یک یا هر دو روش زیر حاصل می‌شود:

الف- فراخوانی سازوکارهای امنیتی به طور مستقیم درون (N)-لایه؛ و/یا

ب- درخواست خدمات محافظتی از (N+1)-لایه. در این مورد حوزه محافظت باید به (N)-خدمت به‌وسیله ترکیب کارکرد قابل اعتماد و/یا سازوکارهای امنیتی خاص در (N)-لایه بسط داده شود.

یادآوری- این موضوع به‌طور ضروری به این معنی نیست که همه کارکردها در (N)-لایه باید قابل اعتماد باشد.

از این رو (N)-لایه تعیین می‌کند که آیا قادر به دستیابی به محافظت مورد نظر درخواست شده است یا نه. اگر قادر به دستیابی به آن نیست، هیچ نمونه‌ای از ارتباط برقرار نخواهد شد.

۶-۲-۲-۱ برقراری یک اتصال (N)-لایه محافظت‌شده

بحث ذیل، فراهم‌سازی خدمات در (N)-لایه (در مقابل رله کردن (N-1)-خدمات) را مورد توجه قرار می‌دهد. در برخی از پروتکل‌های مشخص، برای حصول به یک محافظت مورد نظر رضایت‌بخش، دنباله عملیات زیر ضروری است.

الف- کنترل دسترسی رو به بیرون

(N)-لایه ممکن است کنترل‌هایی را بر روی دسترسی رو به بیرون قرار دهد، یعنی ممکن است به‌صورت محلی (از SMIB) مشخص کند که آیا برقراری (N)-اتصال قابل انجام است یا آنکه ممنوع شده است.

ب- احراز هویت هستار همتا

اگر محافظت مورد نظر شامل احراز هویت هستار همتا است، یا اگر (از SMIB) معلوم شود که (N)-هستار مقصد نیازمند احراز هویت هستار همتا است، آنگاه یک تبادل احراز هویت باید انجام شود. در این کار ممکن است در صورت نیاز دست‌دهی دو یا سه سویه برای فراهم کردن احراز هویت یک‌طرفه یا دوطرفه به‌کار گرفته شود.

گاهی اوقات، تبادل احراز هویت ممکن است در رویه‌های برقراری (N)-اتصال ادغام شده باشد. تحت هر شرایط دیگری، تبادل احراز هویت ممکن است به‌صورت جداگانه از (N)-اتصال انجام شود.

پ- خدمت کنترل دسترسی

(N)-خدمت مقصد یا هستارهای میانی ممکن است محدودیت‌های کنترل دسترسی را به‌کارگیری کنند. اگر اطلاعات خاصی به‌وسیله سازوکار کنترل دسترسی از راه دور مورد نیاز باشد، آنگاه (N)-خدمت آغازگر این اطلاعات را درون پروتکل (N)-لایه یا از طریق کانال‌های مدیریتی فراهم می‌کند.

ت- محرمانگی

اگر خدمت محرمانگی کلی یا انتخابی[1]، انتخاب شده باشد، یک (N)-اتصال محافظت‌شده باید برقرار شود. این کار باید شامل برقراری کلید(های) کاری صحیح و مذاکره پارامترهای رمزنگاشتی برای آن اتصال باشد. این کار ممکن است به‌وسیله تبادل احراز هویت برقرار شده از قبل یا به‌وسیله یک پروتکل مجزا انجام شده باشد.

ث- یکپارچگی داده

اگر یکپارچگی همه (N)-داده‌های کاربر با بازیابی یا بدون آن، یا یکپارچگی فیلدهای انتخابی، انتخاب شده باشد، یک (N)-اتصال محافظت‌شده باید برقرار شود. این اتصال ممکن همان اتصالی باشد که برای فراهم‌سازی خدمت محرمانگی برقرار شود و ممکن است که احراز هویت را فراهم کند. ملاحظات مشابه‌ای برای خدمت محرمانگی برای یک (N)-اتصال محافظت‌شده به‌کارگیری می‌شود.

ج- خدمات انکارناپذیری

اگر خدمت انکارناپذیری با اثبات مبدأ انتخاب شده باشد، پارامترهای رمزنگاری صحیح باید برقرار شوند، یا اینکه یک اتصال محافظت‌شده باید با یک هستار گواهی رسمی برقرار شود.

اگر خدمت انکارناپذیری با اثبات تحویل انتخاب شده باشد، پارامترهای صحیح (که با پارامترهای انکارناپذیری با اثبات مبدأ متفاوت است) باید برقرار شوند، یا اینکه اتصال محافظت‌شده با یک هستار گواهی رسمی باید برقرار شود.

یادآوری- برقراری (N)-اتصال محافظت‌شده ممکن است به‌دلیل فقدان توافق بر روی پارامترهای رمزنگاری (در صورت امکان شامل عدم مالکیت کلیدهای صحیح) یا از طریق رد شدن به‌وسیله یک سازوکار کنترل دسترسی، شکست بخورد.

۶-۲-۳ عملیات یک (N)-اتصال محافظت‌شده

۶-۲-۳-۱ در طول فاز ارسال داده‌ها در یک (N)-اتصال محافظت‌شده، خدمات محافظتی مذاکره‌شده باید فراهم شوند.

آنچه در ادامه در مرز یک (N)-خدمت قابل مشاهده خواهد بود، عبارتند از:

الف- احراز هویت هستار همتا (در بازه‌ها)؛

ب- محافظت از فیلد انتخابی؛ و

پ- گزارش‌کردن یک حمله فعال (به‌عنوان مثال، زمانی که فرابری داده‌ها رخ داده است و خدمت فراهم‌شده یک «خدمت یکپارچگی اتصال بدون بازیابی» است.) (به زیربند ۵-۲-۴-۲ مراجعه شود.)

به‌علاوه موارد زیر نیز ممکن است مورد نیاز باشند:

الف- ثبت کردن دنباله ممیزی امنیت؛ و

ب- تشخیص و سامان‌دهی رویداد.

۶-۲-۳-۲ خدماتی که متمایل به کاربردهای انتخابی هستند عبارتند از:

الف- محرمانگی؛

1 - Total or selective confidentiality Service

ب- یکپارچگی داده (در صورت امکان با احراز هویت)؛ و
پ- انکارناپذیری (به‌وسیله گیرنده یا به‌وسیله فرستنده).

یادآوری ۱ – دو فن برای نشانه‌گذاری اقلام داده‌ای انتخاب‌شده برای کاربرد یک خدمت پیشنهاد شده‌اند. اولین فن شامل نوع‌دهی قوی[1] است. پیش‌بینی می‌شود که لایه ارائه انواع معینی را که نیازمند خدمات محافظتی مشخصی هستند تشخیص دهد. دومین فن، شامل برخی از شکل‌های پرچم‌دهی[2] اقلام داده‌ای مجزا است که باید با خدمات محافظتی مشخص‌شده به‌کار روند.

یادآوری ۲ – فرض بر آن است که یک دلیل برای فراهم ساختن کاربردهای انتخابی خدمات انکارناپذیری ممکن است از سناریوی زیر نشأت بگیرد. برخی از شکل‌های مختلف محاوره مذاکرات بر روی یک ارتباط قبل از توافق دو (N)-خدمت بر سر نگارش نهایی فقره داده‌ای رخ می‌دهد. در آن نقطه، دریافت‌کننده مورد نظر ممکن است از فرستنده درخواست کند که خدمات انکارناپذیری (هم مبدأ و هم تحویل) را بر روی نگارش نهایی توافق‌شده فقره داده‌ای به‌کارگیری کند. فرستنده این خدمات را درخواست کرده و به‌دست می‌آورد، فقره داده‌ای را منتقل می‌کند و سپس اعلامیه اینکه فقره داده‌ای دریافت و توسط گیرنده تصدیق شده است را دریافت می‌کند. خدمات انکارناپذیری هم آغازگر و هم گیرنده فقره داده‌ای را از ارسال موفقیت‌آمیز مطمئن می‌کند.

یادآوری۳ – هر دو نوع خدمت انکارناپذیری (یعنی مبدأ و تحویل) به‌وسیله آغازگر فراخوانی می‌شوند.

۶-۲-۴ فراهم‌سازی انتقال داده‌ها در یک ارتباط بی‌اتصال محافظت‌شده

همه خدمات امنیتی که در پروتکل اتصال‌گرا وجود دارند، در پروتکل‌های بی‌اتصال وجود ندارند. به‌ویژه، محافظت در برابر حملات حذف، درج و بازپخش، اگر مورد نیاز باشند، باید در لایه‌های بالاتر اتصال‌گرا فراهم شوند. محافظت محدود در برابر حملات بازپخش با استفاده از سازوکار مهرزنی زمانی قابل فراهم‌سازی است. به‌علاوه، تعدادی از خدمات امنیتی دیگر قادر به به‌کارگیری درجه مشابه‌ای از امنیت که به‌وسیله پروتکل‌های اتصال‌گرا قابل حصول است، نیستند.

خدمات محافظتی که مناسب انتقال داده‌های بی‌اتصال هستند عبارتند از:

الف- احراز هویت هستار همتا (به زیربند ۵-۲-۱-۱ مراجعه شود.)؛
ب- احراز هویت مبدأ داده‌ها (به زیربند ۵-۲-۱-۲ مراجعه شود.)؛
پ - خدمت کنترل دسترسی (به زیربند ۵-۲-۲ مراجعه شود.)؛
ت - محرمانگی بی‌اتصال (به زیربند ۵-۲-۳-۲ مراجعه شود.)؛
ث - محرمانگی فیلد انتخابی (به زیربند ۵-۲-۳-۳ مراجعه شود.)؛
ج - یکپارچگی بی‌اتصال (به زیربند ۵-۲-۴-۴ مراجعه شود.)؛
چ - یکپارچگی بی‌اتصال فیلد انتخابی (به زیربند ۵-۲-۴-۵ مراجعه شود.)؛ و
ح- انکارناپذیری، مبدأ (به زیربند ۵-۲-۵-۱ مراجعه شود.)

1 - Strong typing
2 - Flagging

خدمات فوق با استفاده از رمزگذاری، سازوکارهای امضا، سازوکارهای کنترل دسترسی، سازوکارهای مسیریابی، سازوکارهای یکپارچگی داده‌ها و/یا سازوکارهای گواهی رسمی، فراهم می‌شوند. (به زیربند ۵-۳ مراجعه شود.)

آغازگر یک انتقال داده‌های بی‌اتصال مجبور به تضمین این است که SDU منفردش دارای همه اطلاعات مورد نیاز برای پذیرفته شدنش در مقصد است.

۷ جای‌گذاری سازوکارها و خدمات امنیتی

این بند خدماتی را تعریف می‌کند که باید در چارچوب مدل مرجع پایه OSI فراهم شده و علاوه بر این روشی را که آن خدمات قابل حصول هستند نیز طرح‌ریزی می‌کند. فراهم‌سازی هر خدمت امنیتی امری اختیاری بوده و به الزامات بستگی دارد.

هرجا یک خدمت امنیتی خاص در این بند شناسایی شده است، طوری که به‌صورت اختیاری به‌وسیله یک لایه خاص فراهم شده باشد، آنگاه آن خدمت امنیتی به‌وسیله سازوکارهای امنیتی که درون آن لایه عمل می‌کند فراهم شده است، مگر آنکه روش دیگری مشخص شده باشد. همان‌گونه که در بند ۶ توضیح داده شد، بسیاری از لایه‌ها، خدمات امنیتی خاص را پیشنهاد می‌کنند. چنین لایه‌هایی ممکن است همواره خدمات امنیتی درون خود را فراهم نسازند اما ممکن است از خدمات امنیتی مناسبی که به‌وسیله لایه‌های پایین‌تر فراهم می‌شوند، استفاده کنند. حتی اگر وقتی که هیچ خدمت امنیتی درون یک لایه فراهم نشود، تعاریف خدمت در آن لایه ممکن است نیاز به تغییراتی داشته باشند تا درخواست‌های خدمات امنیتی به لایه‌های پایین‌تر منتقل شوند.

یادآوری ۱ - سازوکارهای امنیتی فراگیر (به زیربند ۵-۴ مراجعه شود.) در این بند مورد بحث قرار نگرفته‌اند.

یادآوری ۲ - انتخاب مکان قرارگیری سازوکارهای رمزگذاری برای کاربردها در پیوست پ مورد بحث قرار می‌گیرد.

۷-۱ لایه فیزیکی

۷-۱-۱ خدمات

تنها خدمات امنیتی فراهم شده در لایه فیزیکی چه به‌صورت مجزا و چه به‌صورت ترکیبی عبارتند از:

الف- محرمانگی اتصال؛ و

ب- محرمانگی جریان ترافیک.

محرمانگی جریان ترافیک به دو صورت است:

۱- محرمانگی جریان ترافیک کامل که تنها در صورت بروز شرایط خاص می‌تواند فراهم شود، به‌عنوان مثال در ارسال آنی دو سویه، همگام و نقطه به نقطه؛ و

۲- محرمانگی جریان ترافیک محدود که برای سایر انواع انتقالات می‌تواند فراهم شود، به‌عنوان مثال انتقال ناهمگام.

این خدمات امنیتی به محافظت در برابر تهدیدات غیرفعال محدود شده و می‌توانند در ارتباطات نقطه به نقطه و چندهمتایی به‌کارگیری شوند.

۷-۱-۲ سازوکارها

رمزگذاری کامل جریان داده‌ها، سازوکار امنیتی اساسی در لایه فیزیکی است.

یک شکل خاص از رمزگذاری که تنها در لایه فیزیکی قابل کابرد است، امنیت ارسال است. (یعنی امنیت طیف گسترده[1])

محافظت لایه فیزیکی به‌وسیله یک دستگاه رمزگذاری که به‌صورت شفاف عمل می‌کند انجام می‌شود. هدف از محافظت لایه فیزیکی، محافظت از کل جریان بیتی داده‌های خدمت فیزیکی و فراهم کردن محرمانگی جریان ترافیک است.

۷-۲ لایه پیوند داده

۷-۲-۱ خدمات

تنها خدمات امنیتی فراهم شده در این لایه عبارتند از:

الف- محرمانگی اتصال؛ و

ب- محرمانگی بی‌اتصال.

۷-۲-۲ سازوکارها

سازوکار رمزگذاری برای فراهم کردن خدمات امنیتی در لایه پیوند داده مورد استفاده قرار می‌گیرد. (به پیوست پ مراجعه شود.)

کارکرد محافظت امنیتی اضافی برای لایه پیوند قبل از کارکردهای عادی لایه برای ارسال و بعد از کارکردهای لایه عادی برای دریافت انجام می‌شود، به این معنی که سازوکارهای امنیتی کارکردهای لایه عادی را ساخته و از همه کارکردهای لایه عادی استفاده می‌کنند.

سازوکارهای رمزگذاری در لایه پیوند داده به پروتکل‌های لایه پیوند حساس هستند.

۷-۳ لایه شبکه

لایه شبکه به‌صورت درونی برای فراهم‌سازی پروتکل(هایی) برای اجرای عملیات زیر سازمان‌دهی شده است:

الف- دسترسی به زیرشبکه؛

ب- همگرایی وابسته به زیرشبکه؛

پ- همگرایی مستقل از زیرشبکه؛ و

ت- رله و مسیریابی.

(به زیربند ۲-۴ مراجعه شود.)

۷-۳-۱ خدمات

خدمات امنیتی فراهم‌شده به‌وسیله پروتکل‌های اجراکننده کارکردهای دسترسی به زیرشبکه وابسته به فراهم‌سازی خدمت شبکه OSI، عبارتند از:

الف- احراز هویت هستار همتا؛

1 - Spread spectrum security

ب- احراز هویت مبدأ داده‌ها؛
پ- خدمت کنترل دسترسی؛
ت- محرمانگی اتصال؛
ث- محرمانگی بی‌اتصال؛
ج- محرمانگی جریان ترافیک؛
چ- یکپارچگی اتصال بدون بازیابی؛ و
ح- یکپارچگی بی‌اتصال.
این خدمات امنیتی ممکن است به‌صورت مجزا یا به‌صورت ترکیبی فراهم شوند. خدمات امنیتی که ممکن است به‌وسیله پروتکلی فراهم‌شده باشند که عملیات رله و مسیریابی وابسته به فراهم‌سازی خدمت شبکه OSI، از یک سامانه پایانی به یک سامانه پایانی دیگر را انجام می‌دهند با خدماتی که به‌وسیله پروتکلی که عملیات دسترسی به زیرشبکه را انجام می‌دهند، یکسان هستند.

۷-۳-۲ سازوکارها

۷-۳-۲-۱ سازوکارهای امنیتی یکسانی به‌وسیله پروتکل(های) انجام‌دهنده عملیات دسترسی به زیرشبکه، رله و مسیریابی مرتبط با فراهم ساختن خدمت شبکه OSI از یک سامانه پایانی به یک سامانه پایانی دیگر مورد استفاده قرار می‌گیرند. مسیریابی در این لایه انجام می‌شود و بنابراین کنترل مسیریابی نیز در این لایه قرار دارد. خدمات امنیتی شناسایی‌شده به‌صورت زیر فراهم می‌شوند:
الف- خدمت احراز هویت محدودیت همتا به‌وسیله یک ترکیب مناسب از تبادل‌های احراز هویت شده یا محافظت‌شده، تبادل رمز عبور محافظت‌شده و سازوکارهای امضا فراهم می‌شود؛
ب- خدمت احراز هویت مبدأ داده‌ها می‌تواند به‌وسیله سازوکارهای رمزگذاری یا امضا فراهم شود؛
پ- خدمت کنترل دسترسی از طریق استفاده مناسب از سازوکارهای کنترل دسترسی فراهم می‌شود؛
ت- خدمت محرمانگی اتصال به‌وسیله سازوکار رمزگذاری و/یا کنترل مسیریابی فراهم می‌شود.؛
ث- خدمت محرمانگی بی‌اتصال به‌وسیله سازوکار رمزگذاری و/یا کنترل مسیریابی فراهم می‌شود؛
ج- خدمت محرمانگی جریان ترافیک به‌وسیله یک راه‌کار لت‌گذاری ترافیک به همراه یک خدمت محرمانگی در لایه شبکه یا لایه پایین آن و/یا کنترل مسیریابی حاصل می‌شود؛
چ- خدمت یکپارچگی اتصال بدون بازیابی با استفاده از یک سازوکار یکپارچگی داده و برخی اوقات به همراه یک سازوکار رمزگذاری فراهم می‌شود؛ و
ح- خدمت یکپارچگی بی‌اتصال با استفاده از یک سازوکار یکپارچگی داده و برخی اوقات به همراه یک سازوکار رمزگذاری فراهم می‌شود.

۷-۳-۲-۲ سازوکارها در پروتکلی که در عمل دسترسی به زیرشبکه را با فراهم‌سازی خدمت شبکه OSI از یک سامانه پایانی به یک سامانه پایانی دیگر انجام می‌دهد، خدماتی را در سطح زیرشبکه پیشنهاد می‌دهند.
محافظت از یک زیرشبکه که به‌وسیله مدیریت زیرشبکه به‌کارگیری شده است به‌وسیله پروتکل‌های دسترسی به زیرشبکه تحمیل می‌شوند، اما این محافظت‌ها قبل از کارکردهای عادی زیرشبکه در ارسال و بعد از کارکردهای عادی زیرشبکه در دریافت اطلاعات به‌کارگیری می‌شود.

۷-۳-۲-۳ سازوکارهای فراهم‌شده در پروتکل اجراکننده عملیات رله و مسیریابی وابسته به فراهم‌سازی خدمت شبکه OSI، از یک سامانه پایانی به یک سامانه پایانی دیگر، خدماتی را در سطح یک یا چند شبکه دارای اتصال متقابل پیشنهاد می‌دهند.
این سازوکارها قبل از کارکردهای رله و مسیریابی در ارسال و پس از کارکردهای رله و مسیریابی در دریافت مورد نظر قرار می‌گیرند. در مورد سازوکار کنترل مسیریابی، محدودیت‌های مسیریابی مناسب قبل از داده‌ها از SMIB دریافت شده و به همراه محدودیت‌های مسیریابی مورد نیاز به کارکردهای رله و مسیریابی منتقل می‌شوند.

۷-۳-۲-۴ کنترل دسترسی در لایه شبکه می‌تواند اهداف متعددی را دنبال کند. برای مثال، به یک سامانه پایانی امکان کنترل برقراری اتصالات شبکه و رد کردن فراخوانی‌های ناخواسته را می‌دهد. علاوه بر این، به یک یا چند زیرشبکه این امکان را می‌دهد که استفاده از منابع لایه شبکه را کنترل کند. در برخی موارد این هدف مرتبط با تغییر کاربرد شبکه است.

یادآوری– برقراری یک اتصال شبکه اغلب ممکن است نتیجه تغییرات مدیریتی زیرشبکه باشد. حداقل‌سازی هزینه می‌تواند با کنترل کردن دسترسی یا به‌وسیله انتخاب تغییر معکوس یا سایر پارامترهای خاص شبکه انجام شود.

۷-۳-۲-۵ نیازهای یک زیرشبکه خاص ممکن است سازوکارهای کنترل دسترسی را بر روی پروتکلی به‌کارگیری کند که عملیات دسترسی به زیرشبکه را مرتبط با فراهم ساختن خدمت شبکه OSI از یک سامانه پایانی به یک سامانه پایانی دیگر انجام می‌دهد. هنگامی که سازوکارهای کنترل دسترسی به‌وسیله پروتکلی که عملیات مسیریابی و رله را مرتبط با فراهم ساختن خدمت شبکه OSI از یک سامانه پایانی به یک سامانه پایانی دیگر را انجام می‌دهد، فراهم می‌شود، می‌توانند برای کنترل دسترسی به زیرشبکه‌ها و سامانه‌های پایانی مورد استفاده قرار گیرند. آشکارا، حوزه تفکیک کنترل دسترسی به‌طور نسبی بزرگ[1] بوده، و تنها بین هستارهای لایه شبکه قابل تشخیص هستند.

۷-۳-۲-۶ اگر لت‌گذاری ترافیک به همراه یک سازوکار رمزگذاری در لایه شبکه (یا یک خدمت محرمانگی از لایه فیزیکی) مورد استفاده قرار گیرد، آنگاه یک سطح معقول از محرمانگی جریان ترافیک ممکن است حاصل شود.

1 - Coarse

۷-۴ لایه انتقال

۷-۴-۱ خدمات

خدمات امنیتی که به‌صورت انفرادی یا به‌صورت ترکیبی در لایه انتقال فراهم می‌شوند عبارتند از:

الف- احراز هویت هستار همتا؛

ب- احراز هویت مبدأ داده‌ها؛

پ- خدمت کنترل دسترسی؛

ت- محرمانگی اتصال؛

ث- محرمانگی بی‌اتصال؛

ج- یکپارچگی اتصال با بازیابی؛

چ- یکپارچگی اتصال بدون بازیابی؛ و

ح- یکپارچگی بی‌اتصال؛

۷-۴-۲ سازوکارها

خدمات امنیتی شناسایی‌شده که فراهم می‌شوند عبارتند از:

الف- خدمت احراز هویت هستار همتا به‌وسیله ترکیب مناسبی از تبادلات احراز هویت رمزنگاشتی یا محافظت‌شده، تبادل رمز عبور محافظت‌شده و سازوکارهای امضا فراهم می‌شود؛

ب- خدمت احراز هویت مبدأ داده‌ها می‌تواند به‌وسیله رمزگذاری یا سازوکارهای امضا فراهم شود؛

پ- خدمت کنترل دسترسی از طریق استفاده مناسب از سازوکارهای کنترل دسترسی خاص فراهم می‌شود؛

ت- خدمت محرمانگی اتصال به‌وسیله یک سازوکار رمزگذاری فراهم می‌شود؛

ث- خدمت محرمانگی بی‌اتصال به‌وسیله یک سازوکار رمزگذاری فراهم می‌شود؛

ج- خدمت یکپارچگی اتصال با بازیابی با استفاده از یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری فراهم می‌شود؛

چ- خدمت یکپارچگی اتصال بدون بازیابی با استفاده از یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری فراهم می‌شود؛ و

ح- خدمت یکپارچگی بی‌اتصال با استفاده از یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری فراهم می‌شود.

سازوکارهای محافظت به شیوه‌ای عمل می‌کنند که خدمات امنیتی ممکن است برای اتصالات مجزا فراخوانی شوند. برخی اوقات، محافظت به‌گونه‌ای خواهد بود که اتصالات مجزا را می‌توان از سایر اتصالات انتقال تفکیک کرد.

۷-۵ لایه نشست

۷-۵-۱ خدمات

هیچگونه خدمات امنیتی در لایه نشست فراهم نشده است.

۷-۶ لایه ارایه

۷-۶-۱ خدمات

تسهیلاتی به‌وسیله لایه ارائه برای پشتیبانی فراهم‌سازی خدمات امنیتی زیر به‌وسیله لایه کاربرد برای فرایند کاربردی، فراهم *خواهد* شد:

الف- محرمانگی اتصال؛

ب- محرمانگی بی‌اتصال؛ و

پ- محرمانگی فیلد انتخابی.

تسهیلاتی در لایه ارائه همچنین ممکن *است* از فراهم‌سازی خدمات امنیتی زیر به‌وسیله لایه کاربرد برای فرایند کاربردی نیز پشتیبانی کنند:

ت- محرمانگی جریان ترافیک؛

ث- احراز هویت هستار همتا؛

ج- احراز هویت مبدأ داده‌ها؛

چ- یکپارچگی اتصال با بازیابی؛

ح- یکپارچگی اتصال بدون بازیابی؛

خ- یکپارچگی اتصال فیلد انتخابی؛

د- یکپارچگی بی‌اتصال؛

ذ- یکپارچگی بی‌اتصال فیلد انتخابی؛

ر- انکارناپذیری با اثبات منبع؛ و

ز- انکارناپذیری با اثبات تحویل.

یادآوری– تسهیلاتی که به‌وسیله لایه ارائه فراهم می‌شوند آن‌هایی خواهند بود که متکی به سازوکارهایی هستند که تنها بر روی یک نحو انتقال کد کردن داده‌ها می‌توانند عمل کرده و به‌عنوان مثال شامل آن‌هایی خواهند بود که برمبنای فنون رمزنگاری هستند.

۷-۶-۲ سازوکارها

برای خدمات امنیتی زیر، سازوکارهای پشتیبان ممکن است درون لایه ارائه جاسازی شوند و در صورت انجام چنین کاری، ممکن است به همراه سازوکارهای امنیتی لایه کاربرد برای فراهم کردن خدمات امنیتی لایه کاربرد مورد استفاده قرار گیرند:

الف- خدمت احراز هویت هستار همتا می‌تواند با سازوکارهای تبدیل نحوی (مانند رمزگذاری) پشتیبانی شود؛

ب- خدمت احراز هویت مبدأ داده‌ها می‌تواند با سازوکارهای رمزگذاری یا امضا پشتیبانی شود؛

پ- خدمت محرمانگی اتصال می‌تواند با یک سازوکار رمزگذاری پشتیبانی شود؛

ت- خدمت محرمانگی بی‌اتصال می‌تواند با یک سازوکار رمزگذاری پشتیبانی شود؛

ث- خدمت محرمانگی فیلد انتخابی می‌تواند با یک سازوکار رمزگذاری پشتیبانی شود؛

ج- خدمت محرمانگی جریان ترافیک می‌تواند با یک سازوکار رمزگذاری پشتیبانی شود؛
چ- خدمت یکپارچگی اتصال بدون بازیابی می‌تواند با یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری پشتیبانی شود؛
ح- خدمت یکپارچگی اتصال بدون بازیابی می‌تواند با یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری پشتیبانی شود؛
خ- خدمت یکپارچگی بی‌اتصال فیلد انتخابی بدون بازیابی می‌تواند با یک سازوکار یکپارچگی داده برخی اوقات به همراه یک سازوکار رمزگذاری پشتیبانی شود؛
د- خدمت یکپارچگی اتصال فیلد انتخابی می‌تواند با یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری پشتیبانی شود؛
ز- خدمت یکپارچگی بی‌اتصال می‌تواند با یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری پشتیبانی شود؛
ر- خدمت یکپارچگی بی‌اتصال فیلد انتخابی می‌تواند با یک سازوکار یکپارچگی داده‌ها، برخی اوقات به همراه یک سازوکار رمزگذاری پشتیبانی شود؛
ز- خدمت انکارناپذیری با اثبات مبدأ می‌تواند با ترکیب مناسبی از سازوکارهای یکپارچگی داده، امضا و گواهی رسمی پشتیبانی شود؛ و
ژ- خدمت انکارناپذیری با اثبات تحویل می‌تواند با ترکیب مناسبی از سازوکارهای یکپارچگی داده، امضا و گواهی رسمی پشتیبانی شود.
سازوکارهای رمزگذاری به‌کارگیری شده بر روی انتقال‌های داده‌ای هنگامی که در لایه‌های پایانی جای‌گذاری می‌شوند، در لایه ارائه قرار خواهند گرفت.
برخی از خدمات امنیتی در فهرست فوق را می‌توانند با استفاده از سازوکارهای امنیتی که به‌طور کامل در لایه کاربرد وجود دارند، فراهم شوند.
تنها خدمات امنیتی محرمانگی می‌تواند به‌طور کامل به‌وسیله سازوکارهای امنیتی قرارگرفته در لایه ارائه فراهم شوند.
سازوکارهای امنیتی در لایه ارائه به‌عنوان مرحله نهایی تبدیل نحو انتقال در ارسال و مرحله اولیه فرایند تبدیل در دریافت عمل می‌کند.

۷-۷ لایه کاربرد

۱-۷-۷ خدمات

لایه کاربرد یک یا چند خدمت از خدمات پایه‌ای زیر را به‌صورت مجزا یا ترکیبی فراهم می‌کند:
الف- احراز هویت هستار همتا؛
ب- احراز هویت منبع داده‌ها؛
پ- خدمت کنترل دسترسی؛
ت- محرمانگی اتصال؛

ث- محرمانگی بی‌اتصال؛
ج- محرمانگی فیلد انتخابی؛
چ- محرمانگی جریان ترافیک؛
ح- یکپارچگی اتصال با بازیابی؛
خ- یکپارچگی اتصال بدون بازیابی؛
د- یکپارچگی اتصال فیلد انتخابی؛
ذ- یکپارچگی بی‌اتصال؛
ر- یکپارچگی بی‌اتصال فیلد انتخابی؛
ز- انکارناپذیری با اثبات مبدأ؛ و
ژ- انکارناپذیری با اثبات تحویل.

احراز هویت طرف‌های یک ارتباط مورد نظر پشتیبانی از کنترل‌های دسترسی هم به منابع OSI و هم منابع غیر OSI (مانند فایل‌ها، نرم‌افزارها، پایانه‌ها، چاپگرها) در سامانه‌های باز حقیقی را فراهم می‌کنند.

تعیین الزامات امنیتی خاص در هر نمونه از ارتباط، شامل محرمانگی داده‌ها، یکپارچگی و احراز هویت ممکن است به‌وسیله مدیریت امنیت OSI یا مدیریت لایه کاربرد برمبنای اطلاعات موجود در SMIB علاوه بر درخواست‌های انجام شده به‌وسیله فرآیندهای کاربردی انجام شود.

۷-۷-۲ سازوکارها

خدمات امنیتی در لایه کاربرد با استفاده از سازوکارهای زیر فراهم می‌شوند:

الف- خدمت احراز هویت هستار همتا می‌تواند با استفاده از اطلاعات هویتی مبادله‌شده بین هستارهای کاربردی فراهم شود که به‌وسیله سازوکارهای رمزگذاری در لایه ارائه و/یا لایه پایین‌تر محافظت شده است؛

ب- خدمت احراز هویت مبدأ داده‌ها می‌تواند با سازوکارهای امضا یا سازوکارهای رمزگذاری لایه پایین‌تر پشتیبانی شود؛

پ- خدمت کنترل دسترسی آن جنبه‌هایی از یک سامانه باز واقعی که وابسته به OSI هستند، نظیر توانایی ارتباط با سامانه‌های خاص یا هستارهای کاربرد از راه دور می‌تواند به‌وسیله ترکیب سازوکارهای کنترل دسترسی در لایه کاربرد یا لایه‌های پایین‌تر فراهم شود؛

ت- خدمت محرمانگی اتصال می‌تواند با یک سازوکار رمزگذاری لایه پایین‌تر پشتیبانی شود؛

ث- خدمت محرمانگی بی‌اتصال می‌تواند با یک سازوکار رمزگذاری لایه پایین‌تر پشتیبانی شود؛

ج- خدمت محرمانگی فیلد انتخابی می‌تواند با یک سازوکار رمزگذاری در لایه ارائه پشتیبانی شود؛

چ- خدمت محرمانگی جریان ترافیک محدود می‌تواند با یک سازوکار لت‌گذاری ترافیک در لایه کاربرد به همراه خدمت محرمانگی در یک لایه پایین‌تر پشتیبانی شود؛

ح- خدمت یکپارچگی اتصال با بازیابی می‌تواند با استفاده از یک سازوکار یکپارچگی داده لایه پایین‌تر (برخی اوقات به همراه یک سازوکار رمزگذاری) پشتیبانی شود؛

خ- خدمت یکپارچگی اتصال بدون بازیابی می‌تواند با استفاده از یک سازوکار یکپارچگی داده لایه پایین‌تر (برخی اوقات به همراه یک سازوکار رمزگذاری) پشتیبانی شود؛
د- خدمت یکپارچگی اتصال فیلد انتخابی می‌تواند با استفاده از یک سازوکار یکپارچگی داده لایه پایین‌تر (برخی اوقات به همراه یک سازوکار رمزگذاری) پشتیبانی شود؛
ذ- خدمت یکپارچگی بی‌اتصال بدون بازیابی می‌تواند با استفاده از یک سازوکار یکپارچگی داده لایه پایین‌تر (برخی اوقات به همراه یک سازوکار رمزگذاری) پشتیبانی شود؛
ر- خدمت یکپارچگی بی‌اتصال فیلد انتخابی می‌تواند با استفاده از یک سازوکار یکپارچگی داده لایه پایین‌تر (برخی اوقات به همراه یک سازوکار رمزگذاری) پشتیبانی شود؛
ز- خدمت انکارناپذیری با اثبات مبدأ می‌تواند به وسیله ترکیب مناسبی از سازوکارهای امضا و یکپارچگی داده لایه پایین‌تر به همراه یک گواهی رسمی طرف سوم پشتیبانی شود؛ و
ژ- خدمت انکارناپذیری با اثبات تحویل می‌تواند به استفاده از ترکیب مناسبی از سازوکارهای امضا و یکپارچگی داده لایه پایین‌تر به همراه یک گواهی رسمی طرف سوم پشتیبانی شود.
اگر از یک سازوکار گواهی رسمی، برای فراهم‌سازی خدمت انکارناپذیری استفاده شود، به‌صورت یک طرف سوم قابل اعتماد عمل خواهد کرد. ممکن است این سازوکار یک رکورد از واحدهای داده‌ای را به شکل منتقل‌شده (یعنی، طبق نحو انتقال) به‌منظور حل و فصل اختلافات نگه داشته باشد. این سازوکار ممکن است از خدمات محافظت لایه‌های پایین‌تر استفاده کند.

۷-۷-۳ خدمات غیر OSI

فرآیندهای کاربردی خودشان به تنهایی ممکن است به‌طور اساسی همه خدمات را فراهم ساخته و از انواع مشابه‌ای از سازوکارها که در این استاندارد توضیح داده شده، به‌صورتی که به‌طور مناسب در لایه‌های متفاوت معماری جای‌گذاری شده‌اند، استفاده کنند. این نوع استفاده خارج از حوزه بوده، اما با خدمت و تعاریف پروتکل OSI و معماری OSI ناسازگار نیست.

۷-۸ شرح رابطه خدمات امنیتی و لایه‌ها

جدول ۲ لایه‌های مدل مرجع را که در آن‌ها خدمات امنیتی خاص می‌تواند فراهم شود را شرح می‌دهد. توضیحات مربوط به خدمات امنیتی مطابق زیربند ۵-۲ است. توجیه جای‌گذاری یک خدمت در یک لایه خاص مطابق پیوست ب است.

یادآوری ۱- جدول ۲ سعی در تبیین این موضوع که درایه‌های جدول دارای وزن یا اهمیت برابر هستند، نمی کند. برعکس، درجه‌بندی قابل‌ملاحظه مقیاس در درایه‌های جدول وجود دارد.

یادآوری ۲- جای‌گذاری خدمات امنیتی درون لایه شبکه در زیربند ۷-۳-۲ توضیح داده شده است. محل خدمات امنیتی درون لایه شبکه به‌طور قابل ملاحظه‌ای طبیعت و حوزه خدماتی که فراهم خواهند شد را تحت تأثیر قرار می‌دهد.

یادآوری ۳- لایه ارائه شامل شماری از تسهیلات امنیتی است که فراهم‌سازی خدمات امنیتی به‌وسیله لایه کاربرد را پشتیبانی می‌کند.

۸ مدیریت امنیت

۸-۱ کلیات

۸-۱-۱ مدیریت امنیت OSI با جنبه‌هایی از مدیریت امنیت سروکار دارد که با OSI و امنیت مدیریت OSI مرتبط هستند. جنبه‌های مدیریتی امنیت OSI با عملیاتی سروکار دارند که خارج از نمونه‌های عادی ارتباطات بوده، اما نیازمند پشتیبانی و کنترل جنبه‌های امنیتی آن ارتباطات هستند.

یادآوری- دسترس‌پذیری خدمت ارتباطی به‌وسیله طرح شبکه و/یا پروتکل‌های مدیریت شبکه تعیین می‌شود. انتخاب طرح‌های مناسب شبکه و پروتکل‌های مدیریت برای محافظت در برابر انکار خدمت مورد نیاز هستند.

جدول ۲ - رابطه خدمات امنیتی و لایه‌ها

	لایه						
خدمت	۱	۲	۳	۴	۵	۶	۷*
احراز هویت هستار همتا	●	●	بله	بله	●	●	بله
احراز هویت مبدأ داده	●	●	بله	بله	●	●	بله
خدمت کنترل دسترسی	●	●	بله	بله	●	●	بله
محرمانگی اتصال	بله	بله	بله	بله	●	●	بله
محرمانگی بی‌اتصال	●	بله	بله	بله	●	●	بله
محرمانگی میدان منتخب	●	●	●	●	●	●	بله
محرمانگی جریان ترافیک	بله	●	بله	●	●	●	بله
یکپارچگی اتصال با بازیابی	●	●	●	بله	●	●	بله
یکپارچگی اتصال بدون بازیابی	●	●	بله	بله	●	●	بله
یکپارچگی اتصال فیلد انتخابی	●	●	●	●	●	●	بله
یکپارچگی بی‌اتصال	●	●	بله	بله	●	●	بله
یکپارچگی بی‌اتصال فیلد انتخابی	●	●	●	●	●	●	بله
انکارناپذیری، مبدأ	●	●	●	●	●	●	بله
انکارناپذیری، تحویل	●	●	●	●	●	●	بله

کوته‌نوشت‌ها: بله: خدمت باید مطابق با استاندارد برای آن لایه فراهم شود.
● فراهم نشده

* با توجه به لایه ۷ لازم است یادآوری شود که فرآیند کاربردی ممکن است خود آن خدمت امنیتی را فراهم کرده باشد.

۸-۱-۲ خط‌مشی‌های امنیتی متعددی می‌تواند وجود داشته باشد که به‌وسیله مدیر(ان) سامانه‌های باز توزیع‌شده و استانداردهای مدیریت امنیت OSI لازم است از چنین خط‌مشی‌هایی پشتیبانی کنند. هستارهایی که موضوع یک خط‌مشی امنیتی منفرد بوده و به‌وسیله یک مرجع[1] منفرد مدیریت شده‌اند،

1 - Authority

برخی اوقات در آنچه که «دامنه امنیتی[1]» نامیده می‌شوند، جمع‌آوری می‌گردند. دامنه‌های امنیتی و تعامل‌های آن‌ها، ناحیه مهمی برای گسترش‌های آینده هستند.

۸-۱-۳ مدیریت امنیت OSI با مدیریت خدمات و سازوکارهای امنیتی OSI سروکار دارد. چنین مدیریتی به همان اندازه نیازمند توزیع اطلاعات مدیریتی به این خدمات و سازوکارها می‌باشد که نیازمند، جمع‌آوری اطلاعات مربوط به عملیات این خدمات و سازوکارها است. نمونه‌هایی از آن، توزیع کلیدهای رمزنگاشتی، تنظیمات مدیریتی پارامترهای انتخابی امنیتی به‌کارگیری‌شده به‌طور مدیریتی، گزارش رویداد امنیتی هم عادی و هم غیرعادی (دنباله‌های ممیزی) و فعال‌سازی و غیرفعال‌سازی خدمات است. مدیریت امنیت، شامل انتقال اطلاعات مرتبط با امنیت در پروتکل‌هایی می‌شود که خدمات امنیتی خاصی را فراخوانی می‌کنند. (یعنی، در پارامترهای درخواست‌های اتصال)

۸-۱-۴ پایگاه اطلاعات مدیریت امنیت (SMIB) یک منبع انباره[2] مفهومی برای اطلاعات مرتبط با امنیت است که مورد نیاز سامانه‌های باز است. این مفهوم هیچ نوع پیاده‌سازی و چگونگی ذخیره‌سازی آن اطلاعات را مشخص نمی‌کند. اما هر سامانه پایانی باید شامل اطلاعات محلی ضروری باشد تا بتواند خط‌مشی‌های امنیتی مناسبی را به‌کارگیری کند. پایگاه اطلاعات مدیریت امنیت یک پایگاه اطلاعاتی توزیع‌شده است که برای به‌کارگیری یک خط‌مشی امنیتی سازگار (منطقی یا فیزیکی) در یک گروه از سامانه‌های پایانی مورد نیاز است. در عمل، بخش‌هایی از SMIB ممکن است که با MIB ادغام شده یا ممکن است نشده باشد.

یادآوری- محقق‌سازی‌های[3] SMIB متعددی ممکن است وجود داشته باشد، به‌عنوان مثال:

الف- یک جدول از داده‌ها؛

ب- یک فایل؛

ج- داده‌ها یا قواعد توکار شده[4] درون نرم‌افزار یا سخت‌افزار باز سامانه واقعی.

۸-۱-۵ پروتکل‌های مدیریتی، به‌ویژه پروتکل‌های مدیریت امنیت و کانال‌های ارتباطی حامل اطلاعات مدیریتی به‌طور بالقوه آسیب‌پذیر هستند. بنابراین باید توجه ویژه‌ای به تضمین اینکه پروتکل‌ها و اطلاعات مدیریتی محافظت شده‌اند معطوف شود، طوری که محافظت امنیتی فراهم‌شده برای نمونه‌های معمولی ارتباطات تضعیف نشود.

۸-۱-۶ مدیریت امنیت ممکن است نیازمند تبادل اطلاعات مرتبط با امنیت بین مدیران سامانه‌های مختلف باشد، طوری که SMIB بتواند برقرار شده و بسط یابد. در برخی موارد، اطلاعات مرتبط با امنیت از طریق مسیرهای ارتباطی غیر OSI عبور داده می‌شوند و مدیران سامانه‌های محلی از طریق روش‌های غیراستاندارد، SMIB را به‌روزرسانی می‌کنند. در سایر موارد ممکن است تبادل چنین اطلاعاتی بر روی یک مسیر ارتباطی OSI مورد نظر باشد، به‌طوری که اطلاعات بین دو کاربرد مدیریتی امنیت منتقل شود که در

1 - Security domain
2 - Repository
3 - Realizations
4 - Embedded

سامانه‌های باز واقعی اجرا می‌شوند. کاربرد مدیریت امنیت از اطلاعات مراوده‌شده[1] برای به‌روزرسانی SMIB استفاده خواهد کرد. چنین به‌روزرسانی SMIB ممکن است نیازمند احراز هویت قبلی مدیر امنیتی مناسبی باشد.

۸-۱-۷ پروتکل‌های کاربردی برای تبادل اطلاعات مرتبط با امنیت بر روی کانال‌های ارتباطی OSI تعریف خواهند شد.

۸-۲ طبقه‌های مدیریت امنیت OSI

سه طبقه مختلف برای فعالیت‌های مدیریت امنیت OSI وجود دارند که عبارتند از:

الف- مدیریت امنیت سامانه؛

ب- مدیریت خدمت امنیتی؛ و

پ- مدیریت سازوکار امنیتی.

علاوه‌براین، امنیت مدیریت OSI خود نیز باید مورد توجه قرار گیرد. (به زیربند ۸-۲-۴ مراجعه شود.) کارکردهای کلیدی انجام شده به‌وسیله این طبقه‌های مدیریت امنیت در زیر خلاصه شده‌اند.

۸-۲-۱ مدیریت امنیت سامانه

مدیریت امنیت سامانه به مدیریت با جنبه‌های امنیتی مدیریت تمامی محیط OSI سروکار دارد. فهرست فعالیت‌های نوعی[2] که در این طبقه مدیریت امنیت قرار می‌گیرند عبارت است از:

الف- مدیریت کلی خط‌مشی‌های امنیتی که شامل به‌روزرسانی و نگهداشت سازگاری است؛

ب- تعامل با سایر کارکردهای مدیریت OSI؛

پ- تعامل با مدیریت خدمت امنیتی و مدیریت سازوکار امنیتی؛

ت- مدیریت سامان‌دهی رویداد (به زیربند ۸-۳-۱ مراجعه شود.)؛

ث- مدیریت ممیزی امنیت (به زیربند ۸-۳-۲ مراجعه شود.)؛ و

ج- مدیریت بازیابی امنیت (به زیربند ۸-۳-۳ مراجعه شود.).

۸-۲-۲ مدیریت خدمت امنیتی

مدیریت خدمت امنیتی با مدیریت خدمات امنیتی خاص سروکار دارد. فهرست زیر مجموعه‌ای از فعالیت‌های نوعی است که ممکن است در مدیریت یک خدمت امنیتی خاص انجام شود:

الف- تشخیص و نسبت‌دهی محافظت امنیتی مورد نظر برای خدمت؛

ب- نسبت‌دهی و نگهداشت قواعد برای انتخاب (هرجا که جایگزین‌هایی وجود دارد.) سازوکار امنیتی خاص به‌منظور به‌کارگیری در فراهم کردن خدمت امنیتی درخواست‌شده؛

پ- مذاکره (به‌طور محلی و از راه دور) در مورد سازوکارهای امنیتی در دسترس که به توافق مدیریتی قبلی نیاز دارند؛

---

1 - Communicated information

2 - Typical

ت- فراخوانی سازوکارهای امنیتی خاص از طریق کارکرد مدیریت سازوکار امنیتی مناسب، به‌عنوان مثال برای فراهم‌سازی خدمات امنیتی به‌کارگیری‌شده به‌طور مدیریتی؛ و
ث- تعامل با سایر کارکردهای مدیریت خدمت امنیتی و مدیریت سازوکار امنیتی.

۸-۲-۳ مدیریت سازوکار امنیتی

مدیریت سازوکار امنیتی، با مدیریت سازوکارهای امنیتی خاص سروکار دارد. در ادامه یک فهرست نوعی، اما نه جامع، از کارکردهای مدیریتی سازوکار امنیتی آورده می‌شود:
الف- مدیریت کلید؛
ب- مدیریت رمزگذاری؛
پ- مدیریت امضای دیجیتالی؛
ت- مدیریت کنترل دسترسی؛
ث- مدیریت یکپارچگی داده‌ها؛
ج- مدیریت احراز هویت؛
چ- مدیریت لت‌گذاری ترافیک؛
ح- مدیریت کنترل مسیریابی؛ و
خ- مدیریت گواهی رسمی.
هر یک از عملیات مدیریتی سازوکار امنیتی فهرست شده در زیربند ۸-۴ با جزییات بیشتری مورد بحث قرار می‌گیرند.

۸-۲-۴ امنیت مدیریت OSI

امنیت همه کارکردهای مدیریتی OSI و ارتباط اطلاعات مدیریتی OSI قسمت‌های مهم امنیت OSI محسوب می‌شوند. این طبقه از مدیریت امنیت، انتخاب‌های مناسبی از سازوکارها و خدمات امنیتی OSI فهرست شده را به‌منظور تضمین اینکه پروتکل‌ها و اطلاعات مدیریتی OSI به اندازه کافی محافظت‌شده‌اند، فراخوانی می‌کند. (به زیربند ۸-۱-۵ مراجعه شود.) برای مثال، ارتباطات بین هستارهای مدیریتی درگیر پایگاه اطلاعات مدیریت به‌طور کلی نیازمند برخی از شکل‌های محافظت هستند.

۸-۳ فعالیت‌های مدیریت امنیت سامانه مشخص

۸-۳-۱ مدیریت سامان‌دهی رویداد

جنبه‌های مدیریتی سامان‌دهی رویداد قابل مشاهده در OSI شامل گزارش از راه دور تلاش‌های آشکار برای نقض امنیت سامانه و اصلاح آستانه‌های مورد استفاده برای فعال‌سازی گزارش رویداد است.

۸-۳-۲ مدیریت ممیزی امنیت

مدیریت ممیزی امنیت ممکن است شامل موارد زیر باشد:
الف- انتخاب رویدادی که باید ثبت سابقه شده[1] و/یا به‌صورت از راه دور جمع‌آوری شود؛

1 - Logged

ب- فعال و غیرفعال‌سازی ثبت سابقه ممیزی رویدادهای انتخاب شده؛
پ- جمع‌آوری از راه دور رکوردهای ممیزی انتخاب شده؛ و
ت- آماده‌سازی گزارش‌های ممیزی امنیت.

۸-۳-۳ مدیریت بازیابی امنیت

مدیریت بازیابی امنیت ممکن است شامل موارد زیر باشد:
الف- نگهداشت قواعد مورد استفاده برای واکنش در برابر نقض‌های واقعی یا مشکوک امنیت؛
ب- گزارش از راه دور برای تخلفات آشکار امنیت سامانه؛ و
پ- تعامل‌های مدیر امنیتی.

۸-۴ کارکردهای مدیریت سازوکار امنیتی

۸-۴-۱ مدیریت کلید

مدیریت کلید ممکن است شامل موارد زیر باشد:
الف- تولید کلیدهای مناسب در بازه‌های زمانی متناسب با سطح امنیت مورد نیاز؛
ب- تعیین هستارهایی که باید یک نسخه از هر کلید را دریافت کنند، طبق نیازمندی‌های کنترل دسترسی؛
پ- در دسترس قرار دادن یا توزیع کلیدها به روشی امن به نمونه‌های هستار در سامانه‌های باز واقعی.
این گونه فهمیده می‌شود که برخی از کارکردهای مدیریت کلید در خارج از محیط OSI انجام خواهند شد. این مورد شامل توزیع فیزیکی کلیدها به‌وسیله ابزارهای قابل اعتماد است.
تبادل کلیدهای کاری[1] برای استفاده در طول یک همبستگی، یک کارکرد عادی پروتکل لایه است. انتخاب کلیدهای کاری ممکن است با دسترسی به مرکز توزیع کلید یا پیش توزیع از طریق پروتکل‌های مدیریتی نیز انجام شود.

۸-۴-۲ مدیریت رمزگذاری

مدیریت رمزگذاری ممکن است شامل موارد زیر باشد:
الف- تعامل با مدیریت کلید؛
ب- برقراری پارامترهای رمزنگاشتی؛
پ- همزمان‌سازی رمزنگاشتی.
وجود یک سازوکار رمزگذاری به معنی استفاده از مدیریت کلید و راه‌های معمول ارجاع به الگوریتم‌های رمزنگاشتی است.
درجه تمایز محافظت حاصله از طریق رمزگذاری به‌وسیله هستارهایی که درون محیط OSI به‌طور مستقل کلیددهی می‌شوند تعیین می‌شود. این کار، به‌طور کلی، به‌وسیله معماری امنیتی و به‌طور خاص به‌وسیله سازوکار مدیریت کلید تعیین می‌شود.

1 - Working keys

یک مرجع عمومی برای الگوریتم‌های رمزنگاشتی را با استفاده از یک ثبات برای الگوریتم‌های رمزنگاشتی یا پیش توافق‌های بین هستارها می‌توان به‌دست آورد.

۸-۴-۳ مدیریت امضای دیجیتالی

امضای دیجیتالی ممکن است شامل موارد زیر باشد:

الف- تعامل با مدیریت کلید؛

ب- برقراری پارامترها و الگوریتم‌های رمزنگاشتی؛ و

پ- استفاده از پروتکل بین هستارهای ارتباطی و در صورت امکان یک طرف سوم.

یادآوری- به‌طور کلی مشابهت‌های قوی بین مدیریت امضای دیجیتالی و مدیریت رمزگذاری وجود دارد.

۸-۴-۴ مدیریت کنترل دسترسی

مدیریت کنترل دسترسی ممکن است شامل توزیع صفات امنیتی (از جمله رمزهای عبور) یا به‌روزرسانی فهرست کنترل دسترسی یا فهرست‌های قابلیت‌ها باشد. علاوه بر این ممکن است منجر به استفاده از یک پروتکل بین هستارهای ارتباطی و سایر هستارهای فراهم‌کننده خدمات کنترل دسترسی نیز باشد.

۸-۴-۵ مدیریت یکپارچگی داده‌ها

مدیریت یکپارچگی داده‌ها ممکن است شامل موارد زیر شود:

الف- تعامل با مدیریت کلید؛

ب- برقراری پارامترها و الگوریتم‌های رمزنگاشتی؛ و

پ- استفاده از پروتکل بین هستارهای ارتباطی.

یادآوری- هنگام استفاده از فنون رمزنگاشتی برای یکپارچگی داده‌ها، مشابهت‌های قوی بین مدیریت یکپارچگی داده‌ها و مدیریت رمزگذاری وجود دارد.

۸-۴-۶ مدیریت احراز هویت

مدیریت احراز هویت ممکن است منجر به توزیع اطلاعات توصیفی، رمزهای عبور یا کلیدها (با استفاده از مدیریت کلید) به هستارهایی شود که برای انجام عمل احراز هویت مورد نیاز هستند. علاوه بر این ممکن است شامل استفاده از یک پروتکل بین هستارهای ارتباطی و سایر هستارهای فراهم‌کننده خدمات احراز هویت باشد.

۸-۴-۷ مدیریت لت‌گذاری ترافیک

مدیریت لت‌گذاری ترافیک ممکن است شامل نگهداشت قواعدی باشد که برای لت‌گذاری ترافیک مورد نیاز هستند. به‌عنوان مثال ممکن است شامل موارد زیر باشد:

الف- نرخ داده‌ای از پیش تعیین‌شده؛

ب- تعیین نرخ‌های تصادفی داده‌ها؛

پ- تعیین ویژگی‌های پیام نظیر طول؛ و

ت- تغییرپذیری مشخصات، در صورت امکان مطابق با زمان روز و/یا تقویم.

۸-۴-۸ مدیریت کنترل مسیریابی

مدیریت کنترل مسیریابی ممکن است شامل تعریف پیوندها یا زیرشبکه‌هایی باشد که یا امن هستند یا با ملاحظه معیارهای خاصی، قابل اعتماد در نظر گرفته می‌شوند.

۸-۴-۹ مدیریت گواهی رسمی

مدیریت گواهی رسمی ممکن است شامل موارد زیر باشد:

الف- توزیع اطلاعات درباره مراکز گواهی رسمی؛

ب- استفاده از یک پروتکل بین یک مرکز گواهی رسمی و هستارهای ارتباطی؛ و

پ- تعامل با مراکز گواهی رسمی.

پیوست الف

(اطلاعاتی)

اطلاعات پیش زمینه در مورد امنیت در OSI

الف-۱ پیش زمینه

این پیوست موارد زیر را فراهم می‌کند:

الف- اطلاعاتی در مورد امنیت OSI به‌منظور ارائه یک دید کلی نسبت به این استاندارد؛ و

ب- پیش زمینه‌ای در مورد مفاهیم معماری ویژگی‌ها و نیازمندی‌های امنیتی گوناگون.

امنیت در محیط OSI تنها یک جنبه از امنیت پردازش داده‌ها/ارتباطات داده‌ها است. اگر قرار است که امنیت مؤثر باشد، معیارهای محافظتی مورد استفاده در محیط OSI، نیازمند پشتیبانی معیارهایی است که در خارج از OSI وجود دارند. برای مثال اطلاعاتی که بین سامانه‌ها در جریان است ممکن است رمزگذاری شوند، اما اگر هیچ نوع محدودیت امنیتی فیزیکی برای دسترسی به خود سامانه‌ها گذاشته نشود، رمزگذاری بیهوده خواهد بود. همچنین OSI تنها به روابط داخلی سامانه‌ها مربوط می‌شود. برای آنکه ابزارهای امنیتی OSI مؤثر باشند، این ضوابط به همراه ابزارهایی مورد استفاده قرار می‌گیرند که خارج از حوزه OSI هستند.

الف-۲ الزامات امنیتی

الف-۲-۱ از امنیت چه مفهومی برداشت می‌شود؟

عبارت «امنیت» به منظور کمینه‌سازی آسیب‌پذیری‌های منبع و دارایی‌ها مورد استفاده قرار می‌گیرد. هر چیز با ارزشی یک دارایی است. آسیب‌پذیری یک نوع نقطه ضعف بوده که می‌توان از آن برای استفاده غیرقانونی از یک سامانه یا اطلاعات آن سامانه، بهره‌برداری کرد. تهدید[1] یک نقض بالقوه امنیت است.

الف-۲-۲ انگیزه ایجاد امنیت در سامانه‌های باز

سازمان استانداردهای بین‌المللی، نیاز به یک سری از استانداردها را برای بهبود امنیت درون معماری OSI شناسایی کرده است. این موضوع از موارد زیر ناشی شده است:

الف- وابستگی روز افزون جوامع به کامپیوترهایی که به‌وسیله ارتباطات داده‌ای مورد دسترسی واقع‌شده یا مرتبط شده و نیازمند محافظت در برابر تهدیدات مختلف هستند؛

ب- ظهور قانون‌گذاری‌های «محافظت داده‌ها» در برخی کشورها که تهیه کننده‌ها را متعهد می‌سازد که یکپارچگی و حریم خصوصی سامانه ارائه کنند؛ و

پ- تمایل سازمان‌های گوناگون به استفاده از استانداردهای OSI برای سامانه‌های امن موجود یا آینده که در صورت نیاز بهبود داده شده‌اند.

الف-۲-۳ چه چیزی باید محافظت شود؟

به‌طور کلی، موارد زیر نیازمند محافظت هستند:

1 - Threat

الف- اطلاعات و داده‌ها (شامل نرم‌افزار و داده‌های غیرفعال مربوط به ابزارهای امنیتی مانند رمزهای عبور)؛
ب- خدمات پردازش ارتباطی و داده‌ای؛ و
پ- تجهیزات و تسهیلات.

الف-۲-۴ تهدیدات

تهدیدات مربوط به یک سامانه ارتباطات داده‌ای، شامل موارد زیر هستند:
الف- خراب‌کاری عمدی اطلاعات و/یا سایر منابع؛
ب- خراب کردن یا تغییر اطلاعات؛
پ- دزدی، حذف یا از دست دادن اطلاعات و/یا سایر منابع؛
ت- افشای اطلاعات؛ و
ث- وفقه خدمات.
تهدیدات را می‌توان به دو دسته اتفاقی یا عمدی دسته‌بندی کرده و ممکن است فعال یا غیرفعال باشند.

الف-۲-۴-۱ تهدیدات اتفاقی[1]

تهدیدات اتفاقی آن‌هایی هستند که قصد از پیش تعیین‌شده‌ای ندارند. نمونه‌هایی از تهدیدات اتفاقی محقق شده شامل بدعمل کردن سامانه، اشتباهات سهوی عملیاتی و اشکال‌های نرم‌افزاری است.

الف-۲-۴-۲ تهدیدات عمدی[2]

تهدیدات عمدی ممکن است طیف گسترده‌ای از آزمایش‌های اتفاقی با استفاده از ابزارهای نظارتی در دسترس تا حملات پیچیده با استفاده از دانش سامانه‌ای خاص را پوشش دهد. یک تهدید عمدی در صورت محقق شدن، ممکن است یک «حمله» نامیده شود.

الف-۲-۴-۳ تهدیدات غیرفعال

تهدیدات غیرفعال آن‌هایی هستند که در صورت محقق شدن، منجر به تغییر اطلاعات موجود در سامانه‌ها و اطلاعات نگهداری‌شده در سامانه(ها) نمی‌شود و نه عملیات و نه حالت سامانه تغییر نمی‌کند. استفاده از ضبط سرّی مکالمات[3] برای مشاهده اطلاعات ارسالی روی یک خط ارتباطی یک نوع تحقق تهدید غیرفعال است.

الف-۲-۴-۴ تهدیدات فعال[4]

تهدیدات فعال به یک سامانه شامل تغییر اطلاعات نگهداری‌شده در یک سامانه، یا تغییرات حالت یا عملیات آن سامانه است. تغییر بدخواهانه[5] جدول مسیریابی یک سامانه به‌وسیله یک کاربر غیرمجاز نمونه‌ای از یک تهدید فعال است.

1 - Accidental Threats
2 - Intentional Threats
3 - Wiretapping
4 - Active Threats
5 - Malicious

الف-۲-۵ برخی از انواع خاص حمله

آنچه در ادامه می‌آید مرور مختصر برخی از حملات خاص در محیط پردازش داده‌ای ارتباطات داده‌ای است. در بخش‌های آتی، اصطلاحات «مجاز» و «غیرمجاز» ظاهر می‌شوند. عبارت مجازشناسی به معنی اعطاء حقوق است. دو مفهوم از این تعریف برداشت می‌شود: اینکه حقوق، به معنای حقوق برخی فعالیت‌ها (مانند دسترسی به داده‌ها) است و اینکه این حقوق به برخی از هستارها، عامل‌های انسانی، یا فرآیندها اعطاء می‌شود. آنگاه، رفتار مجاز عبارت است از انجام فعالیت‌هایی که حقوق آن‌ها اعطاء شده (و فسخ نشده) است. برای درک بهتر مفهوم مجاز بودن به زیربند الف-۲-۳-۱ مراجعه شود.

الف-۲-۵-۱ دگرنمایی

یک دگرنمایی جایی است که یک هستار طوری وانمود می‌کند که هستار دیگری است. یک دگرنمایی به‌طور معمول به همراه سایر شکل‌های حملات فعال، به‌خصوص بازپخش یا تغییر پیام‌ها استفاده می‌شود. برای مثال می‌توان دنباله‌های احراز هویت را پس از انجام یک دنباله احراز هویت مجاز، اخذ کرده[1] و سپس بازپخش کرد. یک هستار مجاز که حقوق دسترسی[2] کمی دارد می‌تواند با استفاده از دگرنمایی خود را به‌عنوان یک هستار که دارای حقوق دسترسی بیشتری است، معرفی کند.

الف-۲-۵-۲ بازپخش

زمانی که یک پیام یا بخشی از آن برای ایجاد تأثیرات غیرمجاز تکرار می‌شود، بازپخش رخ می‌دهد. برای مثال یک پیام معتبرِ شامل اطلاعات احراز هویت، ممکن است به‌منظور معتبر جلوه دادن خود به‌وسیله یک هستار دیگر، بازپخش شود.

الف-۲-۵-۳ تغییر پیام

تغییر پیام زمانی رخ می‌دهد که محتوای داده‌های انتقالی به‌صورتی غیرمجاز تغییر یابد، بدون اینکه نتایج حاصل از آن تغییر، تشخیص داده شود. به‌عنوان مثال یک پیام به این صورت «به "جان اسمیت" اجازه خواندن فایل محرمانه "حساب‌ها" را بدهید.» به پیام «به "فرد براون" اجازه خواندن فایل محرمانه "حساب‌ها" را بدهید.» تغییر می‌یابد.

الف-۲-۵-۴ انکار خدمت

انکار خدمت زمانی رخ می‌دهد که یک هستار برای اجرای عملیات صحیح خود ناموفق باشد یا از سایر هستارها برای انجام عملیات صحیح خود ممانعت به‌عمل آورد. این حمله ممکن است عمومی باشد، مانند زمانی که یک هستار تمامی پیام‌ها را از بین ببرد، یا اینکه یک هدف مشخص وجود داشته باشد به‌طوری که تمامی پیام‌هایی که به یک مقصد خاص ارسال می‌شوند را از بین ببرد. این حمله ممکن است موجب از بین رفتن ترافیک و/یا ایجاد ترافیک بیش از حد شود. این امکان نیز وجود دارد که پیام‌هایی را ایجاد کند که باعث مختل شدن عملیات شبکه شود، به‌خصوص اگر شبکه هستارهای رله‌ای داشته باشد که تصمیم‌گیری در مورد مسیریابی براساس گزارش‌های مربوط به حالت دریافت‌شده از سایر هستارهای رله را انجام دهند.

---

1 - Capture
2 - Privileges

الف-۲-۵-۵ حملات نفوذگرهای داخلی[1]

این حملات هنگامی رخ می‌دهند که کاربران قانونی یک سامانه به روش‌های ناخواسته یا غیرمجاز عمل کنند. بسیاری از جرائم کامپیوتری شناخته‌شده شامل این حملات است به‌گونه‌ای که امنیت سامانه را به‌خطر انداخته‌اند. روش‌های محافظتی مورد استفاده در برابر این حملات عبارتند از:

الف- بررسی دقیق کارمندان؛

ب- بررسی دقیق سخت‌افزار، نرم‌افزار، خط‌مشی‌های امنیتی و پیکربندی‌های سامانه به‌طوری که این درجه از اطمینان حاصل شود که این موارد به‌درستی عمل می‌کنند (که به‌طور معمول کارکرد قابل اعتماد خوانده می‌شود)؛ و

پ- استفاده دنباله‌های ممیزی برای افزایش احتمال تشخیص چنین حملاتی.

الف-۲-۵-۶ حملات نفوذگرهای خارجی[2]

این حملات ممکن از روش‌هایی شامل موارد زیر استفاده کنند:

الف- شنود (فعال یا غیرفعال)؛

ب- مسدودکردن انتشار[3]؛

پ- دگرنمایی به‌عنوان کاربران مجاز یا مؤلفه‌های مجاز سامانه؛ و

ت- دور زدن سازوکارهای احراز هویت یا کنترل دسترسی.

الف-۲-۵-۷ دریچه تله[4]

هنگامی که یک هستار از سامانه به‌گونه‌ای تغییر می‌یابد که به مهاجم اجازه دهد که اثرات غیرمجازی روی دستورات یا رویداد از پیش تعیین‌شده یا دنباله‌ای از رویدادها داشته باشد، آنگاه گفته می‌شود که یک دریچه تله اتفاق افتاده است. به‌عنوان مثال، تعیین درستی یک رمز عبور می‌تواند به‌گونه‌ای تغییر یابد که علاوه بر عمل عادی خود، رمز عبور یک حمله‌کننده را معتبر محسوب کند.

الف-۲-۵-۸ اسب تروا[5]

هنگامی که به یک سامانه وارد می‌شود، اسب تروا عملی غیرمجاز علاوه بر عمل مجاز دارد. یک رله که نسخه‌هایی از پیام‌ها را برای یک کانال غیرمجاز نیز نسخه‌برداری می‌کند، یک اسب تروا است.

الف-۲-۶ ارزیابی تهدیدات، مخاطره‌ها[6] **و اقدامات در برابر آن‌ها**

ویژگی‌های امنیتی به‌طور معمول هزینه یک سازمان را افزایش داده و ممکن است استفاده از آن را دشوارتر کنند. از این رو قبل از طراحی یک سامانه امن، باید تهدیداتی که نیازمند محافظت در برابر آن‌ها وجود دارد، مشخص شوند.

---

1 - Insider attacks
2 - Outsider attacks
3 - Intercepting Emission
4 - Trapdoor
5 - Trojan horse
6 - Risks

این عمل به‌طور معمول ارزیابی تهدید[1] نامیده می‌شود. یک سامانه به طرق مختلفی آسیب‌پذیراست، اما تنها برخی قابل بهره‌برداری هستند، زیرا حمله‌کننده فرصت کافی نداشته یا به این دلیل که ارزش مخاطره ناشی از شناسایی‌شدن را ندارند. با وجودی که جزییات مسائل مربوط به ارزیابی تهدید خارج از حوزه‌ی این پیوست است، به‌طور کلی می‌توان گفت که شامل موارد زیر است:

الف- تشخیص آسیب‌پذیری‌های سامانه؛

ب- تحلیل احتمال تهدیداتی که قصد بهره‌برداری از این آسیب‌پذیری‌ها را دارند؛

پ- ارزیابی نتایج درصورتی که هر تهدید با موفقیت اجرا شود؛

ت- تخمین هزینه‌ی هر حمله؛

ث- محاسبه‌ی هزینه‌ی اقدامات مقابله بالقوه؛ و

ج- انتخاب سازوکارهای امنیتی که قابل توجیه هستند. (در صورت امکان بااستفاده از تحلیل هزینه-سود)

اقدامات غیرفنی از جمله پوشش بیمه، ممکن است جایگزین‌هایی به صرفه از نظر هزینه برای اقدامات امنیتی فنی باشد. یک امنیت فنی بی عیب و نقص، مانند امنیت فیزیکی بی عیب و نقص، امکان‌پذیر نیست. از این رو، هدف باید این‌گونه باشد که هزینه‌ی انجام یک حمله به اندازه کافی بالا باشد که مخاطره را تا سطوح قابل قبولی کاهش دهد.

الف- ۳ خط مشی امنیتی

این بند، خط‌مشی امنیتی را مورد بحث قرار می‌دهد: نیاز به خط‌مشی امنیتی تعریف‌شده به‌صورت مناسب، نقش آن، رهیافت‌های خط‌مشی مورد استفاده، و پالایش‌ها جهت به‌کارگیری در وضعیت‌های خاص. سپس این مفاهیم برای سامانه‌های ارتباطی به‌کارگیری می‌شوند.

الف-۳-۱ نیاز و مقصود از خط مشی امنیتی

کل حوزه امنیت هم پیچیده و هم دور از دسترس است. هر تحلیل کامل به‌طور منطقی کاملی جزییات گوناگون دلهره‌آوری خواهد داشت. یک خط‌مشی امنیتی مناسب باید توجه خود را به آن جنبه‌هایی از یک وضعیت معطوف کند، که در بالاترین سطح اجازه باید مورد ملاحظه قرار گیرد. به‌طور اساسی، یک خط‌مشی امنیتی به بیان کلی مشخص می‌کند که در طول عملیات یک سامانه چه کارهایی اجازه انجام دارند و چه کارهایی اجازه انجام ندارند. خط‌مشی به‌طور معمول خاص نبوده به این صورت که تنها آنچه را که بالاترین اهمیت را دارد مشخص کرده اما تعیین نمی‌کند که چه نتایجی باید به‌طور دقیق به‌دست آیند. خط‌مشی بالاترین سطح مشخصات امنیتی را تعیین می‌کند.

الف-۳-۲ مفاهیم تعریف خط مشی: فرآیند پالایش

از آن‌جا که خط‌مشی کلی است، نمی‌توان به‌طور واضح و روشن مشخص کرد که چگونه یک خط‌مشی متناسب با یک کاربرد خاص مورد استفاده قرار گیرد. اغلب بهترین روش برای انجام آن اضافه نمودن جزییات بیشتری از کاربرد در هر مرحله برای پالایش خط‌مشی است. برای آگاه شدن از این که جزییات باید چگونه

1 - Threat assessment

باشد، نیازمند مطالعه‌ی ناحیه کاربرد با استفاده از خط‌مشی کلی هستیم. این بررسی‌ها باید مسائلی را مطرح کنند که در سر راه به‌کارگیری شرایط خط‌مشی بر روی کاربرد وجود دارد. فرآیند پالایش منجر به تولید خط‌مشی کلی‌شده که با اصطلاحاتی دقیق با توجه به کاربرد دوباره بیان شده است. این خط‌مشی دوباره بیان شده تعیین جزییات پیاده‌سازی را ساده‌تر می‌کند.

الف-۳ مولفه‌های خط مشی امنیتی

دو جنبه برای خط مشی‌های امنیتی موجود وجود دارد. هر دو جنبه به مفهوم رفتار مجاز بستگی دارند.

الف-۳-۳-۱ مجازشناسی[1]

تهدیداتی که از پیش مورد بحث قرار گرفتند همه با مفهوم رفتارهای مجاز یا غیرمجاز سروکار دارند. بیان اینکه چه چیزی مجازشناسی را تشکیل می‌دهد در خط‌مشی امنیتی قرار داده شده است. یک خط‌مشی امنیتی عام ممکن است بیان کند که: «داده‌ها نباید داده شوند به، مورد دسترسی قرار گیرند به‌وسیله، اجازه استنتاج داشته باشند به‌وسیله، یا نباید هیچ منبعی استفاده شود به‌وسیله، آنهایی که مناسب مجازبودن نیستند». طبیعت مجازشناسی آن است که خط‌مشی‌های مختلف را از هم تمیز می‌دهد. خط‌مشی‌ها را می‌توان براساس ماهیت اجازه مورد استفاده به دو دسته مجزای خط‌مشی‌های مبتنی بر قاعده و مبتنی بر هویت تقسیم‌بندی کرد. اولین دسته از قواعدی مبتنی بر صفات عمومی یا کلاس‌های حساسیت استفاده می‌کنند که به‌صورت سراسری به‌کارگیری می‌شوند. دومی شامل معیارهای مجازشناسی مبتنی بر یک ویژگی منفرد و مشخص است. برخی از ویژگی‌ها برای همیشه به یک هستار منتسب می‌شوند. برخی دیگر ممکن است به‌صورت دارایی‌هایی (مانند قابلیت‌ها) باشند که می‌توانند به هستارهای دیگری منتقل شوند. می‌توان به راحتی خدمت به‌کارگیری شده به‌طور مدیریتی را از خدمت مجازشناسی انتخاب‌شده به‌طور پویا از هم تمیز داد. یک خط‌مشی امنیتی، عناصری از امنیت سامانه را که همیشه به‌کارگیری شده و تأکید می‌شوند (مانند مؤلفه‌های خط‌مشی امنیتی مبتنی بر قاعده و مبتنی بر هویت، اگر وجود داشته باشند.)، و نیز آن‌هایی را که کاربر ممکن است برای استفاده انتخاب نموده تا ببیند که مناسب هستند یا نه، تعیین خواهد کرد.

الف-۳-۳-۲ خط مشی امنیتی مبتنی بر هویت

جنبه‌ی مبتنی بر هویت خط‌مشی‌های امنیتی، به‌طور جزیی، متناظر یک مفهوم امنیتی است که به «نیاز به دانستن» معروف است. هدف، فیلترکردن دسترسی‌ها به داده‌ها و منابع است. به‌طور اساسی، دو روش پایه‌ای پیاده‌سازی خط‌مشی‌های مبتنی بر هویت وجود دارد که به این امر وابسته‌اند که اطلاعات مربوط به حقوق دسترسی به وسیله هستار دسترسی‌یابنده نگهداری می‌شود. یا اینکه بخشی از داده‌هایی است که مورد دسترسی قرار می‌گیرند. مورد قبلی به وسیله ایده‌های حقوق دسترسی و قابلیت‌های داده‌شده به کاربران و مورد استفاده فرآیندهای عمل‌کننده از طرف آن‌ها به کمک مثال فهمانده می‌شود. فهرست‌های کنترل دسترسی (ACLs) مثالی از روش دوم هستند. در هر دو مورد، اندازه‌ی واحد داده‌ای (از یک فایل کامل

1 - Authorization

گرفته تا یک عنصر داده‌ای) که ممکن است در یک قابلیت آمده باشد یا اینکه در فهرست کنترل دسترسی حمل شود، ممکن است خیلی متغیر[1] باشد.

الف-۳-۳-۳ خط‌مشی امنیتی مبتنی بر قاعده

مجازشناسی در یک خط‌مشی امنیتی مبتنی بر قاعده به‌طور معمول براساس حساسیت است. در یک سامانه امن، داده‌ها و/یا منابع باید با استفاده از برچسب‌های امنیتی نشانه‌گذاری شوند. فرآیندهای عمل‌کننده از طرف کاربران انسانی ممکن است برچسب امنیتی مناسب با آغازکنندگان خود را دریافت کنند.

الف-۳-۴ خط‌مشی امنیتی، ارتباطات و برچسب‌ها

مفهوم برچسب‌دهی در محیط‌های ارتباطی داده‌ای مفهومی مهم است. برچسب‌های حمل‌کننده صفات مختلف، نقش‌های مختلفی را بازی می‌کنند. واحدهای داده‌ای وجود دارند که در طی یک ارتباط جابه‌جا می‌شوند، فرآیندهایی وجود دارند که ارتباط را شروع می‌کنند، و هستارهایی نیز وجود دارند که پاسخ می‌دهند و کانال‌ها و منابع دیگری از سامانه نیز وجود دارند که در طول ارتباط مورد استفاده قرار می‌گیرند. در همگی آن‌ها ممکن است به طریقی ویژگی‌هایشان به آن‌ها برچسب‌دهی شوند. خط‌مشی‌های امنیتی باید مشخص کنند که چگونه صفات هر یک برای فراهم‌سازی امنیت لازمه، مورد استفاده قرار می‌گیرند. ممکن است که لازم باشد تا برای برقراری مفاد امنیتی صحیح صفات برچسب‌دهی شده نیاز به مذاکره باشد. هنگامی که برچسب‌های امنیتی هم به فرآیندهای دسترسی‌یابنده و هم به داده‌های مورد دسترسی پیوست می‌شوند، اطلاعات اضافی مورد نیاز برای به‌کارگیری کنترل دسترسی مبتنی بر هویت باید به برچسب‌ها مرتبط باشند. هنگامی که خط‌مشی امنیتی مبتنی بر هویت کاربر دسترسی‌یابنده به داده‌ها، یا به‌صورت مستقیم یا از طریق یک فرآیند، باشد، آنگاه برچسب‌های امنیتی باید حاوی اطلاعاتی در مورد هویت کاربر باشند. قواعد برچسب‌های خاص باید در یک خط‌مشی امنیتی موجود در پایگاه اطلاعات مدیریت امنیت (SMIB) و/یا از طریق مذاکره با سامانه‌های پایانی بیان شوند. برچسب ممکن است با صفاتی پسوندگذاری‌شده باشد که حساسیت برچسب را تعیین می‌کند، اطلاعات نهان[2] اداره کردن و توزیع را مشخص می‌کند، زمانبندی و وضع[3] را محدود می‌کند، و الزامات خاص سامانه پایانی را می‌نویسد.

الف-۳-۴-۱ برچسب‌های فرآیند

در احراز هویت، هویت شناسی[4] کامل آن دسته از فرآیندها یا هستارهای آغازگر و پاسخ‌گو به یک نمونه ارتباط، به همراه تمامی صفات مناسب، به نوعی از اهمیت پایه‌ای برخوردارند. بنابراین، SMIBها حاوی اطلاعات کافی درباره‌ی صفاتی خواهند بود که برای هر خط‌مشی به‌طور مدیریتی به‌کارگیری شده، مهم است.

1 - Highly variable
2 - Coverts
3 - Disposition
4 - Identification

الف-۳-۴-۲ برچسب‌های داده‌ها

از آن‌جا که واحدهای داده‌ای در طول ارتباط جابه‌جا می‌شوند و هر یک به‌شدت به برچسب خود وابسته می‌شوند (این وابسته‌سازی مهم بوده و در برخی نمونه‌های خط‌مشی‌های مبتنی بر قاعده، الزام است که برچسب به یک بخش خاص از فقره داده‌ای[1] برچسب شود، قبل از آنکه به کاربرد ارائه شود). فنونی که برای حفظ یکپارچگی فقره داده‌ای به‌کار می‌روند، دقت[2] و پیوستگی[3] برچسب‌ها را نیز حفظ می‌کند. این صفات به‌وسیله کارکردهای کنترل مسیریابی در لایه‌ی پیوند داده‌ی مدل مرجع پایه OSI می‌توانند مورد استفاده قرار گیرند.

الف-۴ سازوکارهای امنیتی

یک خط‌مشی امنیتی ممکن است با استفاده از سازوکارهای مختلفی، به‌صورت منفرد یا ترکیبی، بسته به اهداف یا سازوکارهای مورد استفاده، پیاده‌سازی شود. به‌طور کلی، یک سازوکار به یکی از سه کلاس (دارای همپوشانی) زیر تعلق دارد:

الف- پیشگیری؛

ب- تشخیص؛ و

پ- بازیابی.

سازوکارهای امنیتی مناسب برای محیط‌های ارتباط داده‌ای در ادامه مورد بحث قرار می‌گیرند.

الف-۴-۱ فنون رمزنگاشتی و رمزگذاری

رمزنگاری زمینه‌ی بسیاری از خدمات و سازوکارهای امنیتی است. کارکردهای رمزنگاری ممکن است به‌عنوان جزیی از رمزگذاری، رمزگشایی، یکپارچگی داده‌ها، تبادل احراز هویت، بررسی و ذخیره‌ی رمز عبور و غیره مورد استفاده قرار گیرند تا برای رسیدن به محرمانگی، یکپارچگی و احراز هویت کمک کنند. رمزگذاری مورد استفاده برای محرمانگی، داده‌های حساس (یعنی، داده‌هایی که باید محافظت شوند.) را به داده‌های با حساسیت کمتر تبدیل می‌کند. هنگامی که برای یکپارچگی یا احراز هویت مورد استفاده قرار می‌گیرد، فنون رمزنگاشتی برای محاسبه کارکردهای غیرقابل جعل استفاده می‌شوند.

رمزگذاری در حالت اولیه بر روی یک متن واضح اجراشده تا یک متن رمزشده را به‌وجود آورد. نتیجه‌ی رمزگشایی، یا متن واضح است یا متن رمزشده‌ای است که تحت لفافه‌هایی[4] قرار دارد. از نظر محاسباتی، امکان‌پذیر[5] است که از متن واضح برای پردازش‌های همه منظوره‌ای استفاده کرد که محتوای معنایی آن در دسترس خواهد بود. جز از راه‌های خاص (مثل رمزگشایی اولیه یا تطابق دقیق)، از نظر محاسباتی پردازش متن رمزشده امکان‌پذیر نیست، زیرا محتوی آن مخفی است. برخی اوقات رمزگذاری، به‌طور عمدی

1 - Data item
2 - Accuracy
3 - Coupling
4 - Cover
5 - Feasible

برگشت‌ناپذیر است (برای مثال، به‌وسیله کوتاه کردن یا از دست دادن داده‌ها)، مواقعی که حتی به‌دست آوردن متن واضح اصلی، مانند رمزهای عبور، دلخواه نیست.

کارکردهای رمزنگاری از متغیرهای رمزنگاشتی[1] استفاده نموده و بر روی فیلدها، واحدهای داده‌ای، و/یا جریان‌هایی از واحدهای داده‌ای کار می‌کنند. دو متغیر رمزنگاری یکی کلید است که تبدیل‌های خاص را هدایت می‌کند و دیگری متغیر مقداردهی اولیه است که برای حفظ تصادفی بودن متن رمزشده در برخی پروتکل‌های رمزنگاری خاص مورد نیاز است. کلید باید همواره محرمانه باقی مانده و هم کارکرد رمزنگاری و هم متغیر مقداردهی اولیه ممکن است باعث افزایش تأخیر و مصرف پهنای باند شوند. این امر، افزودنی‌های رمزنگاشتی «شفاف» یا «کوتاه مدت[2]» سامانه‌های موجود را پیچیده می‌کنند.

متغیرهای رمزنگاشتی می‌توانند برای هر دو روش رمزگذاری و رمزگشایی، به‌صورت متقارن یا نامتقارن باشند. کلیدهایی که در الگوریتم‌های نامتقارن استفاده می‌شوند، به‌صورت ریاضی با همدیگر رابطه دارند در حالی که یکی را نمی‌توان از روی دیگری به‌دست آورد. این الگوریتم‌ها را به‌طور معمول الگوریتم‌های «کلید عمومی» می‌نامند چرا که یک کلید را می‌توان عمومی اعلام کرد در حالی که دیگری سرّی باقی می‌ماند.

وقتی که از نظر محاسباتی بازیابی متن واضح از متن رمزشده بدون دانستن کلید، عملی است متن رمزشده ممکن است تحلیل رمز[3] شود. این امر زمانی رخ می‌دهد که از کارکردهای رمزنگاشتی ضعیف و معیوبی استفاده شده باشد. انسداد و تحلیل ترافیک می‌توانند منجر به حملاتی به سامانه‌ی رمزنگاشتی شود که شامل درج، تغییر یا حذف پیام، ارسال مجدد متن رمزشده‌ای که از پیش دریافت‌شده و دگرنمایی است. بنابراین، پروتکل‌های رمزنگاشتی طوری طراحی می‌شوند که در برابر حملات و گاهی اوقات، تحلیل ترافیک، مقاومت کنند. یک ابزار متقابل در برابر تحلیل ترافیک خاص، «محرمانگی جریان ترافیک» نامیده می‌شود، که هدف آن پنهان کردن وجود یا عدم وجود داده‌ها و ویژگی‌های آن است. اگر متن رمزشده رله شود، آدرس باید در رله‌کننده‌ها و دروازه‌ها[4] واضح (رمزنشده) باشد. اگر داده‌ها تنها در هر پیوند ارتباطی رمز شده باشند و در رله‌کننده‌ها و دروازه‌ها رمزگشایی‌شده (و بنابراین آسیب‌پذیر) باشند، معماری از روشی موسوم به «رمزگذاری پیوند به پیوند[5]» استفاده می‌کند. اگر فقط آدرس (داده‌های کنترلی مشابه) در رله‌ها دروازه‌ها واضح باشد، معماری از روشی موسوم به «رمزگذاری انتها به انتها[6]» استفاده می‌کند. از دیدگاه امنیت، استفاده از رمزگذاری انتها به انتها دلخواه است، اما به‌طور کامل از نظر معماری تا حد قابل ملاحظه‌ای پیچیده‌تر است به‌خصوص اگر توزیع کلید الکترونیکی داخل باند[7] (یک کارکرد مدیریت کلید) را نیز شامل شود. رمزگذاری‌های پیوند به پیوند و انتها به انتها برای حصول برخی اهداف امنیتی ممکن است با یکدیگر ترکیب شوند. یکپارچگی داده اغلب با محاسبه‌ی یک مقدار وارسی رمزنگاشتی انجام می‌شود. این مقدار وارسی ممکن است در یک یا چند مرحله به‌دست آید که نتیجه‌ی عملیات ریاضی بر روی متغیرهای

1 - Cryptovariables
2 - Drop-in
3 - Cryptanalysis
4 - Gateways
5 - Link-by-link Encipherment
6 - End-to-end Encipherment
7 - In-band electronic key distribution

رمزنگاشتی و داده‌ها است. این مقدار به داده‌هایی که باید محافظت شوند مرتبط می‌شود. این مقادیر گاهی اوقات «کدهای تشخیص فرابری[1]» نامیده می‌شوند.

فنون رمزنگاشتی می‌توانند برای فراهم‌سازی یا کمک به فراهم‌سازی محافظت در برابر موارد زیر استفاده شوند:

الف- مشاهده جریان پیام و/یا تغییر آن؛

ب- تحلیل ترافیک؛

پ- انکار؛

ث- جعل؛

ج- اتصال غیرمجاز؛ و

چ- تغییر پیام‌ها.

الف-۴-۲ جنبه‌های مدیریت کلید

استفاده از الگوریتم‌های رمزنگاشتی، استفاده از روش‌های مدیریت کلید را نیز مشخص می‌کند. مدیریت کلید، تولید، توزیع و کنترل کلیدهای رمزنگاشتی را شامل می‌شود. انتخاب یک روش مدیریت کلید مبتنی است بر ارزیابی شرکت‌کنندگان محیطی که قرار است آن روش در آن محیط استفاده شود. ملاحظات مربوط به این محیط شامل تهدیداتی که باید در برابر آن‌ها محافظت شود (هم داخلی به سازمان و هم خارجی)، فناوری‌های مورد استفاده، ساختار معماری، ساختار فیزیکی و مکان فراهم‌کنندگان خدمت رمزنگاشتی است.

نکاتی که در زمینه مدیریت کلید باید به آن‌ها توجه کرد عبارتند از:

الف- استفاده از «طول عمر[2]» مبتنی بر زمان، میزان استفاده یا سایر معیارهای تعریف‌شده برای هر کلید به‌صورت صریح یا ضمنی؛

ب- شناسایی صحیح کلیدها مطابق کارکردشان، طوری که استفاده از آن‌ها ممکن است فقط برای کارکردشان رزرو شده باشد، به‌عنوان مثال کلیدهایی که برای استفاده برای خدمت محرمانگی مورد استفاده قرار می‌گیرند نباید بتوانند برای خدمت یکپارچگی استفاده شوند و بالعکس؛

پ- ملاحظات غیر OSI، مانند توزیع فیزیکی و بایگانی کلیدها.

نکاتی که در زمینه مدیریت کلید الگوریتم‌های کلید متقارن باید به آن‌ها توجه کرد عبارتند از:

الف- استفاده از یک خدمت محرمانگی در پروتکل مدیریت کلید برای حمل کلیدها؛

ب- استفاده از یک سلسله مراتب کلید. موقعیت‌های مختلف باید مجاز باشند که عبارتند از:

۱- سلسله مراتب‌های «افقی[3]» که تنها از کلیدهای رمزگذاری داده‌ای[4] استفاده می‌کنند، به‌صورت ضمنی یا صریح از یک مجموعه از هویت یا شاخص کلیدها انتخاب می‌شوند؛

۲- سلسله مراتب‌های چندلایه‌ای کلید[5]؛

1 - Manipulation detection codes.
2 - Lifetime
3 - Flat
4 - Data-encrypting keys
5 - Multilayer key hierarchies

۳- کلیدهای رمزگذاری کلید[1] هرگز نباید برای محافظت از داده‌ها استفاده شده و کلیدهای رمزگذاری داده هرگز نباید برای محافظت کلیدهای رمزگذاری کلید استفاده شوند.

پ- تقسیم مسئولیت‌ها به‌گونه‌ای که هیچ فردی نسخه‌ای کامل از یک کلید مهم را نداشته باشد.

نکاتی که در زمینه الگوریتم‌های مدیریت کلید نامتقارن باید به آن‌ها توجه کرد عبارتند از:

الف- استفاده از خدمت محرمانگی در پروتکل مدیریت کلید برای انتقال کلیدهای سری؛ و

ب- استفاده از یک خدمت یکپارچگی یا انکارناپذیری با اثبات مبدأ در پروتکل مدیریت کلید برای حمل کلیدهای عمومی. این خدمات ممکن است از طریق استفاده از الگویتم‌های رمزنگاشتی متقارن و/یا نامتقارن فراهم شوند.

الف-۴-۳ سازوکارهای امضای دیجیتالی

اصطلاح امضای دیجیتالی برای مشخص کردن یک فن خاص استفاده می‌شود که برای فراهم کردن خدمات امنیتی، مانند انکارناپذیری و احراز هویت، به‌کار می‌رود. سازوکارهای امضای دیجیتالی نیازمند استفاده از الگوریتم‌های رمزنگاشتی نامتقارن هستند. ویژگی اساسی سازوکار امضای دیجیتالی آن است که واحدهای داده‌ای امضا شده را نمی‌توان بدون استفاده از کلید خصوصی ایجاد کرد. این به معنای آن است که:

الف- یک داده امضا شده نمی‌تواند به‌وسیله هیچ کسی جز آن کسی که کلید خصوصی را دارد، تولید شود.

ب- دریافت‌کننده نمی‌تواند واحد داده‌ای امضا شده را تولید کند.

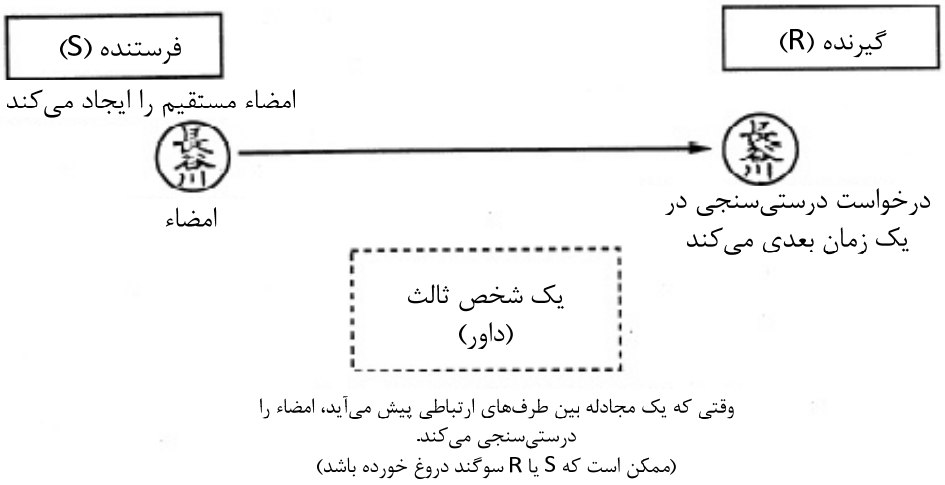
از این رو، با استفاده از اطلاعاتی که در دسترس عموم قرار دارند می‌توان به‌طور یکتا امضاکننده داده‌ها که دارنده‌ی کلید خصوصی است را شناسایی کرد. درمورد ب می‌توان هویت امضاکننده را از طریق یک طرف سوم مورد اعتماد اثبات کرد، که در مورد مجاز بودن واحد داده امضا شده قضاوت می‌کند. این نوع امضای دیجیتالی را طرح امضای مستقیم[2] می‌نامند. (به شکل ۱ مراجعه شود.) در سایر موارد، بخش پ نیز باید در نظر گرفته شود:

پ- فرستنده نمی‌تواند ارسال داده امضاشده را انکار کند.

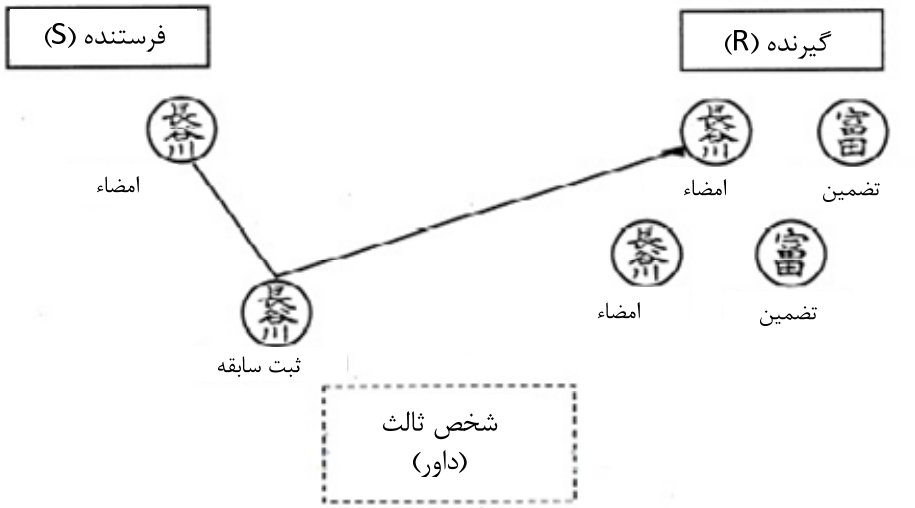
یک طرف سوم قابل اعتماد (داور) منبع و یکپارچگی را به دریافت‌کننده ثابت می‌کند. این روش امضای دیجیتالی گاهی اوقات طرح داوری‌شده امضا نامیده می‌شود. (به شکل ۲ مراجعه شود.)

یادآوری- فرستنده ممکن است نیازمند آن باشد که دریافت‌کننده، دریافت داده‌های امضاشده را انکار نکند. این عمل را می‌توان با استفاده از خدمت انکارناپذیری با اثبات ارسال با استفاده از یک ترکیب مناسب از سازوکارهای امضای دیجیتالی، یکپارچگی داده و گواهی رسمی انجام داد.

1 - Data-encrypting keys
2 - Direct signature scheme



شکل ۱ - طرحی از امضای مستقیم



یک طرف سوم منبع را احراز هویت نموده (و به دریافت‌کننده تضمین می‌دهد (مثلاً یک نتیجه مثبت)). اطلاعات مورد نیاز برای اثبات منبع و جامعیت داده به وسیله یک شخص ثالث در سابقه ثبت می‌شود. در این حالت، S سپس نمی‌تواند ارسال موفقیت‌آمیز واحد داده‌ای امضاءشده را منکر شود.

شکل ۲ - طرحی از امضای غیرمستقیم

الف-۴-۴ سازوکارهای کنترل دسترسی

سازوکارهای کنترل دسترسی سازوکارهایی هستند که برای به‌کارگیری یک خط‌مشی به‌منظور محدود کردن دسترسی به منابع، به جز برای کاربرانی که مجاز هستند به‌کار می‌رود. فنونی شامل استفاده از فهرست‌ها یا ماتریس‌های کنترل دسترسی (که به‌طور معمول شامل هویت‌های اقلام کنترل‌شده و کاربران مجاز، مانند

اعضا و فرآیندها است.)، رمزهای عبور، قابلیت‌ها، برچسب‌ها یا نشانه‌ها، و دارایی‌هایی که مشخص‌کننده حقوق دسترسی باشند، می‌شود. هر جایی که از قابلیت‌ها استفاده می‌شود، باید غیرقابل جعل بوده و به روشی قابل اعتماد حمل شوند.

الف-۴-۵ سازوکارهای یکپارچگی داده

سازوکارهای یکپارچگی داده بر دو نوع است: آن‌هایی که برای محافظت از یکپارچگی یک واحد داده‌ای منفرد استفاده می‌شوند و آن‌هایی که برای محافظت از هم یکپارچگی یک واحد داده‌ای منفرد و هم ترتیب کل جریان داده‌ای در یک اتصال مورد استفاده قرار می‌گیرند.

الف-۴-۵-۱ تشخیص تغییر در جریان پیام

فنون تشخیص تخریب که به‌طور معمول به تشخیص خطاهای بیتی، خطاهای بستک[1] و خطاهای ترتیب‌دهی[2] که به‌وسیله پیوندها و شبکه‌های ارتباطی به‌وجود آمده‌اند، مربوط می‌شوند. اما اگر سرآیندها و پی‌آیندهای[3] پروتکل با استفاده از سازوکارهای یکپارچگی محافظت نشده باشند، یک نفوذگر مطلع می‌تواند به‌راحتی و باموفقیت این وارسی‌ها را دور بزند. از این رو تشخیص موفق تغییر جریان پیام تنها با استفاده از فنون تشخیص تخریب به همراه اطلاعات ترتیب قابل انجام دادن است. این روش از تغییر در جریان پیام جلوگیری نمی‌کند اما می‌تواند آگاه‌سازی از وقوع حملات را فراهم کند.

الف-۴-۶ سازوکارهای تبادل احراز هویت

الف-۴-۶-۱ انتخاب سازوکار

انتخاب‌ها و ترکیبات زیادی از سازوکارهای تبادل احراز هویت وجود دارند که برای اهداف خاصی مناسب هستند. به‌عنوان مثال می‌توان به موارد زیر اشاره کرد:

الف- هنگامی که هستارهای همتا و ابزارهای ارتباطی هر دو قابل اعتماد هستند، هویت‌شناسی هستار همتا را می‌توان با یک رمز عبور انجام داد. رمز عبور از بروز خطا جلوگیری کرده، اما اثباتی در برابر بدخواهی[4] نیست (به ویژه، نه در برابر بازپخش). احراز هویت دوطرفه را می‌توان با استفاده از رمز عبور مجزا در هر جهت انجام داد.

ب- هنگامی که هر هستار به هستار همتای خود اعتماد دارد اما به ابزار ارتباطی اعتماد ندارد، محافظت در برابر حملات فعال را می‌توان با ترکیباتی از رمزهای عبور و رمزگذاری یا با ابزارهای رمزنگاشتی انجام داد. محافظت در برابر حمله بازپخش نیازمند دست‌دهی[5] دو طرفه است. احراز هویت دوطرفه با محافظت در برابر حمله بازپخش را می‌توان با استفاده از دست‌دهی سه طرفه انجام داد.

پ- اگر موجویت‌ها به هستارهای همتا یا ابزارهای ارتباطی اعتماد ندارند، (یا احساس می‌کنند که در آینده نمی‌توانند اعتماد داشته باشند.) می‌توان از خدمات انکارناپذیری استفاده کرد. از این خدمات با استفاده از

1 - Block
2 - Sequencing
3 - Trailers
4 - Malevolence
5 - Handshaking

سازوکارهای امضای دیجیتالی و/یا گواهی رسمی می‌توان استفاده کرد. این سازوکارها را می‌توان به همراه سازوکارهای قسمت ب مورد استفاده قرار داد.

الف-۴-۷ سازوکارهای لت‌گذاری ترافیک

ایجاد ترافیک جعلی و لت‌گذاری واحدهای داده‌ای پروتکل با اندازه مشخص می‌تواند محافظت محدودی را در برابر تحلیل ترافیک فراهم سازد. برای موفقیت، سطح ترافیک جعلی باید تقریباً برابر بالاترین سطح ترافیک پیش‌بینی‌شده باشد. علاوه بر این، واحدهای داده‌ای پروتکل باید رمزگذاری و رمزگشایی شوند به‌طوری که تشخیص ترافیک جعلی امکان‌پذیر نبوده و تفاوت آن با ترافیک واقعی محسوس نباشد.

الف-۴-۸ راه کار کنترل مسیریابی

مشخصات هشدارهای مسیریابی برای انتقال داده (شامل مشخصات کامل یک مسیر) ممکن است برای حصول اطمینان از اینکه داده‌ها تنها بر روی مسیرهایی منتقل می‌شوند که از نظر فیزیکی امن بوده یا حصول اطمینان از اینکه اطلاعات حساس تنها بر روی مسیرهایی با سطح محافظت مناسب منتقل می‌شوند، مورد استفاده قرار گیرند.

الف-۴-۹ سازوکار گواهی رسمی[1]

سازوکار گواهی رسمی مبتنی بر مفهوم طرف سوم قابل اعتماد (یک مرجع گواهی رسمی) است که برای مطمئن ساختن از خصوصیت‌های معینی درباره اطلاعات مبادله‌شده بین دو هستار، مانند مبدأ، یکپارچگی، یا زمان ارسال و دریافت آن‌ها مورد استفاده قرار می‌گیرد.

الف-۴-۱۰ امنیت فیزیکی و کارکنان

ابزارهای امنیت فیزیکی همواره برای حصول اطمینان از امنیت کامل، ضروری هستند. امنیت فیزیکی پرهزینه بوده و به‌طور معمول فعالیت‌های این حوزه برای حداقل‌سازی نیاز به آن با استفاده از روش‌های دیگر (ارزان‌تر) است. ملاحظات امنیت کارکنان و فیزیکی خارج از حوزه OSI بوده، اگر چه همه‌ی سامانه‌ها در نهایت به شکلی به امنیت فیزیکی و اعتمادپذیری کارکنان عمل‌کننده در سامانه اعتماد می‌کند. رویه‌های عملیاتی موجود برای انجام عملیات صحیح و تعیین مسئولیت‌های کارکنان باید تعریف شده باشند.

الف-۴-۱۱ سخت‌افزار/نرم‌افزار قابل اعتماد

روش‌های مورد استفاده برای حصول اطمینان از کارکرد صحیح یک هستار شامل روش‌های اثبات صوری، درستی‌سنجی و اعتبارسنجی، تشخیص و ثبت سوابق حملات شناخته‌شده انجام شده و ساخت هستار به‌وسیله کارکنان قابل اعتماد در یک محیط امن است. اقدامات احتیاطی برای حصول اطمینان از اینکه هستار به‌صورت اتفاقی یا عمدی تغییر داده نشده طوری که امنیت را در طول عمر عملیاتی‌اش مصالحه نکند[2] نیز مورد نیاز است، به‌عنوان مثال در طول زمان نگهداشت یا ارتقاء. برخی هستارها در سامانه باید مورد

1 - Notarization
2 - Compromise

اعتماد باشند تا اگر قرار است امنیت حفظ شود نیز به‌طور صحیح کار کنند. روش‌هایی که برای ایجاد اعتماد به‌کار می‌روند خارج از حوزه OSI هستند.

پیوست ب

(اطلاعاتی)

توجیه جای‌گذاری سازوکارها و خدمات امنیتی در بند ۷

ب-۱ کلیات

این پیوست دلایل فراهم‌سازی خدمات امنیتی شناسایی‌شده در لایه‌های مختلف را که در بند ۷ تعیین شده‌اند ذکر می‌کند. اصول لایه‌بندی امنیت که در زیربند ۶-۱-۱ این استاندارد شناسایی شد، این فرآیند انتخاب را مدیریت کرده است.

یک خدمت امنیتی خاص می‌تواند به‌وسیله بیش از یک لایه فراهم شود، چرا که تأثیر هر یک بر روی کلیت امنیت ارتباطی می‌تواند متفاوت در نظر گرفته شود (به‌عنوان مثال محرمانگی اتصال در لایه‌های ۱ و ۴). بدون توجه به این امر با توجه به کارکردهای ارتباطی داده‌ای OSI موجود (مانند رویه‌های چند پیوندی، کارکردهای هم‌تافتگری[1]، راه‌های مختلف بهبود خدمت بی‌اتصال به یک خدمت اتصال‌گرا) و برای اینکه به سازوکارهای انتقال داده اجازه‌ی عمل داده، ممکن است ضروری باشد که به یک خدمت خاص اجازه داده شود که در لایه‌های دیگر نیز فراهم شود، با وجودی که تأثیر آن بر امنیت متفاوت در نظر گرفته شده باشد.

ب-۲ احراز هویت هستار همتا

لایه‌های ۱ و ۲: خیر، احراز هویت هستار همتا در این لایه‌ها مفید به نظر نمی‌رسد.

لایه ۳: بله، روی زیرشبکه‌های منفرد و برای مسیریابی و/یا ارتباطات بین‌شبکه‌ای.

لایه ۴: بله، احراز هویت یک سامانه پایانی به سامانه پایانی دیگر در لایه ۴ می‌تواند برای احراز هویت متقابل برای دو یا چند هستار نشست، قبل از برقراری اتصال و در طول برقراری آن اتصال مورد استفاده قرار گیرد.

لایه ۵: خیر، به نظر می‌رسد که فراهم کردن این خدمت در لایه ۵ و لایه‌های بالاتر سودی نداشته باشند.

لایه ۶: خیر، اما سازوکارهای رمزگذاری می‌توانند از این خدمت در لایه کاربرد پشتیبانی کنند.

لایه ۷: بله، احراز هویت هستار همتا باید به‌وسیله لایه کاربرد فراهم شود.

ب-۳ احراز هویت مبدأ داده‌ها

لایه‌های ۱ و ۲: خیر، احراز هویت مبدأ داده‌ها در این لایه‌ها مفید به نظر نمی‌رسد.

لایه ۳ و ۴: احراز هویت مبدأ داده‌ها می‌تواند به‌صورت انتها به انتها در مسیریابی و رله لایه ۳ و/یا در لایه ۴ به‌صورت زیر فراهم شوند:

الف- فراهم سازی احراز هویت هستار همتا در زمان برقراری اتصال به همراه احراز هویت پیوسته مبتنی بر رمزگذاری در طول برقراری اتصال، به‌صورت بالفعل[2] خدمت احراز هویت مبدأ داده‌ها را فراهم می‌کنند.

---

1 - Multiplexing

2 - de facto

ب- حتی جایی که (الف) موجود نباشد، احراز هویت مبدأ داده‌ها مبتنی بر رمزگذاری را می‌توان با کمی سربار اضافی برای سازوکارهای یکپارچگی داده از پیش جاسازی‌شده در این لایه‌ها فراهم کرد.
لایه ۵: خیر، فراهم کردن این خدمت در لایه ۴ یا لایه ۷ سودی ندارد.
لایه ۶: خیر، اما سازوکارهای رمزگذاری در لایه کاربرد، این خدمت را پشتیبانی می‌کنند.
لایه ۷: بله، در صورت امکان به همراه سازوکارهایی در لایه ارایه.

ب-۴ کنترل دسترسی

لایه‌های ۱ و۲: سازوکارهای کنترل دسترسی را نمی‌توان در لایه‌های ۱ و ۲ در یک سامانه که با تمامی پروتکل‌های OSI مطابقت دارد فراهم کرد، از آنجایی که هیچ تسهیلات پایانی برای چنین سازوکاری در دسترس نیست.
لایه ۳: سازوکارهای کنترل دسترسی ممکن است به وسیله الزامات یک زیرشبکه خاص بر روی نقش دسترسی به زیرشبکه تحمیل شوند. هنگام اجرا به وسیله نقش رله و مسیریابی، سازوکارهای دسترسی در لایه شبکه را می‌توان هم برای کنترل دسترسی‌ها به زیرشبکه‌ها با استفاده از هستارهای رله و هم برای کنترل دسترسی سامانه‌های پایانی، مورد استفاده قرار داد. به‌طور واضح، در صورتی که دسترسی‌ها دانه‌دانه و قابل تفکیک باشند، تنها تمایز بین هستارهای لایه شبکه امکان‌پذیر خواهد بود.
برقراری یک اتصال شبکه ممکن است اغلب منجر به مسئولیت‌هایی برای مدیر زیرشبکه شود. حداقل‌سازی هزینه را می‌توان با کنترل کردن دسترسی و انتخاب مسئولیت‌های معکوس یا سایر پارامترهای خاص شبکه یا زیرشبکه انجام داد.
لایه ۴: بله، می‌توان از سازوکارهای کنترل دسترسی در یک اتصال انتقالی انتها به انتها استفاده کرد.
لایه ۵: خیر، فراهم‌سازی این سازوکار در لایه ۴ یا لایه ۷ سودی نخواهد داشت.
لایه ۶: خیر، این سازوکار برای لایه ۶ مناسب نیست.
لایه ۷: بله، پروتکل‌ها یا فرآیندهای کاربردی می‌توانند تسهیلات کنترل دسترسی کاربردگرا را فراهم سازند.

ب-۵ محرمانگی همه (N)-داده‌های کاربر در یک (N)-اتصال

لایه ۱: بله، از آن‌جا که درج الکتریکی زوج‌های شفاف ابزارهای تبدیل می‌تواند محرمانگی کامل را به یک اتصال فیزیکی بدهد، باید در این لایه فراهم شود.
لایه ۲: بله، اما هیچ سود امنیتی بیشتری از محرمانگی در لایه‌های ۱ یا ۳ ندارد.
لایه ۳: بله، برای نقش دسترسی به زیرشبکه روی زیرشبکه‌های مجزا و برای نقش‌های مسیریابی و رله روی بین‌شبکه‌ها.
لایه ۴: بله، چرا که اتصال انتقالی مجزا منجر به یک سازوکار انتقال انتها به انتها شده و می‌تواند اتصالات مربوط به جلسات را تفکیک کند.
لایه ۵: خیر، چرا که هیچ سودی برای محرمانگی در لایه‌های ۳ و ۴ و ۷ ندارد. به نظر می‌رسد فراهم کردن این خدمت در این لایه مناسب نباشد.
لایه ۶: بله، چرا که سازوکارهای رمزگذاری باعث فراهم شدن تبدیلات نحوی خالص می‌شوند.

لایه ۷: بله، به همراه سازوکارهایی که در لایه‌های پایین‌تر وجود دارند.

ب-۶ محرمانگی تمامی (N)-داده‌های کاربر در یک (N)-SDU مجزا و بی‌اتصال

توجیه مربوط می‌شود به محرمانگی تمامی (N)-داده‌های کاربر جز برای لایه ۱ جایی که هیچ خدمت بدون اتصالی وجود ندارد.

ب-۷ محرمانگی فیلدهای انتخابی در (N)-داده‌های کاربر از یک SDU

این خدمت محرمانگی به وسیله رمزگذاری در لایه‌ی ارائه فراهم شده و به وسیله سازوکارهایی در لایه‌ی کاربرد مطابق معنای داده‌ها مورد استفاده قرار می‌گیرد.

ب-۸ محرمانگی جریان ترافیک

محرمانگی جریان ترافیک فقط می‌تواند در لایه ۱ به‌دست آید. این امر با درج فیزیکی یک زوج وسیله رمزگذاری در مسیر انتقال فیزیکی به‌دست می‌آید. فرض بر آن است که مسیر انتقال یک مسیر دو طرفه همزمان و همگام بوده، طوری که درج لوازم، تمامی انتقالات روی رسانه فیزیکی را غیر قابل تشخیص می‌کند.

بالای لایه فیزیکی، امنیت ترافیک کامل امکان‌پذیر نیست. برخی از تأثیرات آن می‌تواند به‌علت استفاده از محرمانگی SDU کامل در یک لایه و تزریق ترافیک جعلی در لایه بالاتر باشد. این چنین سازوکاری هزینه‌بر بوده و به‌طور بالقوه مقدار زیادی از ظرفیت راه‌گزینی و حامل را مصرف خواهد کرد.

اگر محرمانگی جریان ترافیک در لایه ۳ فراهم شده باشد، لت‌گذاری ترافیک یا کنترل مسیریابی مورد استفاده قرار خواهد گرفت. کنترل مسیریابی ممکن است منجر به ایجاد محرمانگی جریان ترافیک محدود شود که این کار به‌وسیله مسیردهی پیام‌ها در اطراف زیرشبکه‌ها یا پیوندهای ناامن انجام می‌شود. اما استفاده همزمان از لت‌گذاری ترافیک در لایه ۳ استفاده بهتر از شبکه را در پی خواهد داشت برای مثال با اجتناب از لت‌گذاری و تراکم شبکه غیرضروری.

محرمانگی جریان ترافیک محدود در لایه کاربرد می‌تواند با تولید ترافیک جعلی به همراه محرمانگی برای جلوگیری از شناسایی ترافیک جعلی فراهم شود.

ب-۹ یکپارچگی همه (N)-داده‌های کاربر برروی یک (N)-اتصال (با بازیابی خطا)

لایه‌های ۱ و ۲: لایه‌های ۱ و ۲ قادر به فراهم کردن این خدمت نیستند. لایه ۱ هیچ سازوکار تشخیص یا بازیابی ندارد و سازوکار لایه ۲ تنها برمبنای نقطه به نقطه عمل خواهد کرد، نه برمبنای انتها به انتها و از این رو برای فراهم‌سازی این خدمت مناسب نیست.

لایه ۳: خیر، چرا که دسترسی به بازیابی خطا وجود ندارد.

لایه ۴: بله، چرا که یک اتصال لایه انتقال انتها به انتهای صحیح را فراهم می‌کند.

لایه ۵: خیر، چرا که بازیابی خطا یکی از عملیات لایه ۵ نیست.

لایه ۶: خیر، اما سازوکارهای رمزگذاری قادر به پشتیبانی از این خدمت در لایه کاربرد هستند.

لایه ۷: بله، به همراه سازوکارهای موجود در لایه ارایه.

ب-۱۰ یکپارچگی همه (N)-داده‌های کاربر بر روی یک (N)-اتصال (بدون بازیابی خطا)

لایه‌های ۱و ۲: لایه‌های ۱ و ۲ قادر به فراهم کردن این خدمت نیستند. لایه ۱ هیچ سازوکار تشخیص یا بازیابی ندارد و سازوکار لایه ۲ تنها برمبنای نقطه به نقطه عمل خواهد کرد، نه برمبنای انتها به انتها و از این رو برای فراهم‌سازی این خدمت مناسب نیست.

لایه ۳: بله، برای نقش دسترسی به زیرشبکه روی زیرشبکه‌های مجزا و برای نقش‌های مسیریابی و رله در بین شبکه.

لایه ۴: بله، برای مواردی که برقراری ارتباط پس از تشخیص یک حمله فعال قابل قبول باشد.

لایه ۵: خیر، چرا که هیچ سودی برای یکپارچگی داده‌ها در لایه‌های ۳ و ۴ یا ۷ ندارد.

لایه ۶: خیر، اما سازوکارهای رمزگذاری قادر به پشتیبانی از این خدمت در لایه کاربرد هستند.

لایه ۷: بله، به همراه سازوکارهای موجود در لایه ارایه.

ب-۱۱ یکپارچگی فیلدهای انتخابی درون (N)-داده‌های کاربر یک (N)-SDU منتقل‌شده بر روی یک (N)-اتصال (بدون بازیابی)

یکپارچگی فیلد انتخابی را می‌توان با سازوکارهای رمزگذاری در لایه ارائه به همراه فراخوانی و بررسی سازوکارهای لایه کاربرد فراهم کرد.

ب-۱۲ یکپارچگی همه (N)-داده‌های کاربر در یک (N)-SDU بی‌اتصال منفرد

به‌منظور حداقل کردن تکرار عملیات، یکپارچگی انتقال‌های بی‌اتصال تنها در همان لایه‌هایی باید فراهم شود که یکپارچگی بدون بازیابی را فراهم می‌کنند. به‌عنوان نمونه می‌توان به لایه‌های کاربرد، انتقال و شبکه اشاره کرد. این سازوکارهای یکپارچگی دارای اثرات بسیار محدودی هستند و این امر باید مد نظر قرار گیرد.

ب-۱۳ یکپارچگی فیلدهای انتخابی در یک (N)-SDU بی‌اتصال منفرد

یکپارچگی فیلدهای انتخابی را می‌توان با سازوکارهای رمزگذاری در لایه ارائه به همراه فراخوانی و بررسی سازوکارهای لایه کاربرد فراهم کرد.

ب-۱۴ انکارناپذیری

خدمات انکارناپذیری مبدأ و تحویل را می‌توان با استفاده از سازوکار گواهی رسمی که شامل یک رله در لایه ۷ است فراهم کرد.

استفاده از امضای دیجیتالی برای انکارناپذیری نیازمند همکاری نزدیک لایه‌های ۶ و ۷ با همدیگر است.

پیوست پ

(اطلاعاتی)

انتخاب مکان رمزگذاری برای کاربردها

پ-۱ بسیاری از کاربردها به رمزگذاری در بیش از یک لایه نیاز ندارند. انتخاب لایه نیازمند موارد مهمی است که در زیر توضیح داده خواهند شد.

۱- اگر به محرمانگی جریان ترافیک کامل نیاز است، رمزگذاری در لایه فیزیکی یا امنیت انتقال (برای مثال، فنون طیف گسترده مناسب) انتخاب می‌شوند. امنیت کافی لایه فیزیکی و مسیریابی قابل اعتماد و کارکرد مشابه می‌تواند تمامی نیازهای محرمانگی در رله‌ها را برآورده کند.

۲- اگر دانه‌بندی بالایی از محافظت (یعنی به‌طور بالقوه یک کلید جداگانه برای هر ارتباطات کاربردی) و انکارناپذیری یا محافظت فیلد انتخابی نیاز باشد، آنگاه رمزگذاری در لایه ارائه انتخاب خواهد شد. محافظت از فیلد انتخابی به دلیل استفاده زیاد الگوریتم‌های رمزگذاشتی از توان، مسئله‌ای مهم است. رمزگذاری در لایه ارائه منجر به فراهم شدن یکپارچگی بدون بازیابی، انکارناپذیری و تمامی انواع محرمانگی می‌شود.

۳- اگر محافظت دسته‌ای ساده از سامانه پایانی به ارتباطات پایانی و/یا وسیله رمزگذاری خارجی مد نظر باشد (به‌عنوان مثال، به‌منظور ایجاد محافظت فیزیکی از الگوریتم و کلیدها یا محافظت در برابر نرم‌افزارهای خطادار)، آنگاه رمزگذاری لایه شبکه انتخاب خواهد شد. این امر موجب ایجاد محرمانگی و یکپارچگی بدون بازیابی می‌شود.

یادآوری- با وجودی که بازیابی در لایه شبکه فراهم نمی‌شود، سازوکارهای بازیابی عادی در لایه انتقال برای بازیابی از حملات تشخیص داده شده، به وسیله لایه شبکه مورد استفاده قرار می‌گیرند.

۴- اگر یکپارچگی با بازیابی به همراه دانه‌بندی بالای محافظت مورد نیاز باشد، آنگاه رمزگذاری در لایه انتقال انتخاب خواهد شد. این کار می‌تواند موجب فراهم شدن محرمانگی و یکپارچگی با یا بدون بازیابی شود.

۵- رمزگذاری در لایه پیوند داده برای پیاده‌سازی‌های آتی توصیه نمی‌شود.

پ-۲ هنگامی که دو یا چند مورد از این مسایل کلیدی مدنظر هستند، رمزگذاری ممکن است در بیش از یک لایه مورد نیاز باشد.