ISIRI
11210-2
1st. edition

جمهوری اسلامی ایران
Islamic Republic of Iran
مؤسسه استاندارد وتحقیقات صنعتی ایران
Institute of Standards and Industrial Research of Iran

استاندارد ملی ایران
۱۱۲۱۰-۲
چاپ اول

فناوری اطلاعات– فنون امنیتی– امنیت شبکه فناوری اطلاعات قسمت ۲: معماری امنیتی شبکه

Information technology - Security techniques - IT network security Part 2: Network security architecture

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران
تهران - خیابان ولیعصر، ضلع جنوبی میدان ونک، پلاک ۱۲۹۴، صندوق پستی: ۶۱۳۹-۱۴۱۵۵
تلفن: ۵-۸۸۸۷۹۴۶۱
دورنگار: ۸۸۸۸۷۰۸۰ و۸۸۸۸۷۱۰۳
کرج - شهر صنعتی، صندوق پستی ۱۶۳-۳۱۵۸۵
تلفن: ۸- ۲۸۰۶۰۳۱(۰۲۶۱))
دورنگار: ۲۸۰۸۱۱۴ (۰۲۶۱)
پیام نگار: standard@isiri.org.ir
وب‌گاه : www.isiri.org
بخش فروش، تلفن: ۲۸۱۸۹۸۹ (۰۲۶۱) ، دورنگار: ۲۸۱۸۷۸۷ (۰۲۶۱)
بها: ۴۱۲۵ ریال

Institute of Standards and Industrial Research of IRAN
Central Office: No.1294 Valiaser Ave. Vanak corner, Tehran, Iran
P. O. Box: 14155-6139, Tehran, Iran
Tel: +98 (21) 88879461-5
Fax: +98 (21) 88887080, 88887103
Headquarters: Standard Square, Karaj, Iran
P.O. Box: 31585-163
Tel: +98 (261) 2806031-8
Fax: +98 (261) 2808114
Email: standard @ isiri.org.ir
Website: www.isiri.org
Sales Dep.: Tel: +98(261) 2818989, Fax.: +98(261) 2818787
Price: 4125 Rls.

به‌نام خدا

آشنایی با مؤسسهٔ استاندارد و تحقیقات صنعتی 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.

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان مؤسسه* 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 ذیصلاح 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 شود که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که مؤسسه استاندارد تشکیل می‌دهد به تصویب رسیده باشد.

مؤسسهٔ استاندارد و تحقیقات صنعتی 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 پیشرفتهای علمی، فنی و صنعتی جهان و استانداردهای بینالمللی بهره‌گیری می‌شود.

مؤسسهٔ استاندارد و تحقیقات صنعتی 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 کشو ر و / یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. مؤسسه 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 سا زمانها 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 ، مؤسسهٔ استاندارد 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 آنها 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 مؤسسه است.

---

* موسسهٔ استاندارد و تحقیقات صنعتی ایران

1- International organization for Standardization
2 - International Electro technical Commission
3- International Organization for Legal Metrology (Organization International de Metrology Legal)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

"فناوری اطلاعات– فنون امنیتی– امنیت شبکه فناوری اطلاعات ، قسمت ۲: معماری امنیتی شبکه "

رئیس:	**سمت و/یا نمایندگی**
صلاحی، احمد (دکتری کامپیوتر)	مدیر گروه فناوری امنیت شبکه مرکز تحقیقات مخابرات ایران
دبیر:	
برزگر، مریم (کارشناسی ارشد مهندسی کامپیوتر)	کارشناس مرکز تحقیقات مخابرات ایران
اعضاء:	
بحری، پیمان (کارشناسی ارشد مهندسی کامپیوتر- سخت‌افزار)	کارشناس مرکز تحقیقات مخابرات ایران
پیلتن، علیرضا (کارشناسی مهندسی کامپیوتر)	کارشناس شرکت امن‌افزار گستر شریف
تدین، محمد حسام (دکتری ریاضی)	هیات علمی پژوهشکده امنیت مرکز تحقیقات مخابرات ایران
حبیبی، هاشم (کارشناسی ارشد مهندسی کامپیوتر)	سازمان هوا فضا
حقیقی، صیاد (کارشناسی‌ارشد مهندسی برق- مخابرات/ امن)	دانشگاه خواجه نصیرالدین طوسی
خسروی، رامین (کارشناسی‌ارشد مهندسی برق- مخابرات/ میدان)	کارشناس مرکز تحقیقات مخابرات ایران
خلاش قزل‌احمد، سمیه (کارشناسی ارشد ریاضی)	کارشناس مرکز تحقیقات مخابرات ایران
رستم‌پور، سهراب (کارشناسی مهندسی برق)	کارشناس مسئول شبکه شرکت ارتباطات سیار

رنجکش، نازی (کارشناسی ارشد مهندسی برق- مخابرات/ میدان)	کارشناس مرکز تحقیقات مخابرات ایران
سهی‌زاده ابیانه، محمدرضا (کارشناسی ارشد مهندسی برق- مخابرات/ امن)	کارشناس صنایع الکترونیک زعیم
سیفی، مهرداد (کارشناسی ارشد مدیریت صنعتی)	کارشناس و مسئول تدوین استانداردهای امنیت شبکه شرکت ارتباطات سیار
صابری، جواد (کارشناسی ارشد مهندسی برق- مخابرات/ امن)	مرکز تحقیقات مخابرات امن
طباطبائی، سید امیر حسین (کارشناسی ارشد ریاضی)	کارشناس صنایع الکترونیک زعیم
عظیمی، پدرام (کارشناسی ارشد مهندسی برق- مخابرات)	کارشناس دفتر تدوین شرکت مخابرات ایران
عنایتی، علیرضا (کارشناسی‌ارشد مهندسی برق- مخابرات/ سیستم)	کارشناس مرکز تحقیقات مخابرات ایران
کاظمی، سمیه (کارشناسی ارشد مهندسی برق- مخابرات/ میدان)	کارشناس مرکز تحقیقات مخابرات ایران
میراسکندری، سیدمحمدرضا (کارشناسی مهندسی برق)	مدیر کل شرکت فناوری اطلاعات
میرقدری، عبدالرسول (دکتری آمار)	هیات علمی دانشگاه امام حسین
نوروزی، سعید (کارشناسی کامپیوتر/ نرم‌افزار)	رئیس اداره شبکه شرکت ارتباطات سیار
یادگاری، امیرمنصور (کارشناسی ارشد مهندسی برق- مخابرات/ میدان)	هیات علمی پژوهشکده امنیت مرکز تحقیقات مخابرات ایران

فهرست مندرجات

ادامه فهرست مندرجات

پیش گفتار

این استاندارد تحت عنوان " فناوری اطلاعات– فنون امنیتی– امنیت شبکه فناوری اطلاعات، قسمت ۲: معماری امنیتی شبکه" که پیش نویس آن درکمیسیون‌های مربوط توسط مؤسسهٔ استاندارد و تحقیقات صنعتی ایران و مرکز تحقیقات مخابرات ایران تهیه و تدوین شده و در شصت و پنجمین اجلاس کمیتهٔ ملی استاندارد رایانه و فرآوری داده‌ها مورخ ۸۷/۱۱/۲۷ مورد تصویب قرار گرفته است، اینک به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود .

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت های ملی و جهانی در زمینهٔ 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 تجدیدنظر استانداردهای ملی استفاده کرد.

منابع و ماخذی که برای تهیهٔ این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 18028-1:2006, Informaation technology – Security techniques – IT network security – Part 2: Network security architecture

مقدمه

صنایع مربوط به IT و ارتباطات راه دور، به‌دنبال راه‌حل‌های امنیتی فراگیر و مقرون به صرفه هستند. یک شبکه امن بایستی در برابر حملات مخرب و ناخواسته، حفاظت شود و نیازهای کسب و کار را از لحاظ محرمانگی، یکپارچگی، دسترسی‌پذیری، انکارناپذیری، پاسخگوئی، اعتبار و قابلیت اطمینان اطلاعات و سرویس‌ها، برآورده سازد. امن‌سازی یک شبکه به‌منظور حفظ دقت در صدور صورت‌حساب‌ها یا استفاده از اطلاعات مناسب نیز ضروری است. قابلیت‌های امنیتی محصولات، در امنیت کلی شبکه (شامل کاربردها و سرویس‌ها) تاثیرگذار است. از طرفی هر میزان که محصولات بیشتری به‌منظور فراهم نمودن راه‌حل‌های جامع با هم ترکیب شوند، قابلیت همکاری این محصولات یا فقدان آن‌ها، میزان موفقیت راه‌حل را تعیین خواهد نمود. امنیت تنها نباید برای هر محصول یا سرویس درنظر گرفته شود، بلکه باید به‌گونه‌ای توسعه یابد که قابلیت ترکیب توانایی‌های امنیتی را در کلیه راه‌حل‌های انتها به انتها ارتقا بخشد. بنابراین هدف استاندارد ISO/IEC 18028 ارایه راهنمائی‌هایی دقیق در زمینه جنبه‌های مدیریتی، عملیاتی و کاربردی شبکه‌های IT و اتصالات متقابل آنها است. اشخاصی که درون یک سازمان مسوول امنیت IT به‌طور کلی و امنیت شبکه‌های IT به‌طور خاص هستند، بایستی قادر باشند به‌منظور برآوردن نیازمندی‌های خاص خود، موارد مطرح‌شده در استاندارد ISO/IEC 18028 را برآورده سازند. اهداف اصلی این استاندارد عبارتند از:

- در این استاندارد تعریف و توصیف مفاهیم مرتبط با امنیت شبکه و راهنمایی‌های مدیریتی آن، شامل چگونگی شناسایی و تحلیل عوامل مرتبط با ارتباطات که به‌منظور تعیین نیازهای امنیتی شبکه درنظر گرفته می‌شوند، به انضمام ارایه مقدمه‌ای بر حیطه‌های ممکن کنترلی و حیطه‌های فنی خاص (که در قسمت‌های بعدی استاندارد ISO/IEC 18028 بررسی می‌شوند)،
- در قسمت دوم این استاندارد تعریف یک معماری امنیتی استاندارد که چارچوبی سازگار برای پشتیبانی از برنامه‌ریزی، طراحی و پیاده‌سازی امنیت شبکه است،
- در استاندارد ISO/IEC 18028-3، تعریف فنون ایمن‌سازی جریان‌های اطلاعات بین شبکه‌ها با استفاده از دروازه‌های امنیتی،
- در استاندارد ISO/IEC 18028-4، تعریف فنون ایمن‌سازی دسترسی راه دور،
- در استاندارد ISO/IEC 18028-5، تعریف فنون ایمن‌سازی اتصالات بین شبکه‌ای که توسط VPNها ایجاد می‌شوند.

قسمت اول این استاندارد مربوط به کسانی است که مالک، اپراتور و یا استفاده‌کننده از یک شبکه هستند. این افراد علاوه بر مدیران و مجریانی که مسوولیت‌های خاصی در زمینه امنیت اطلاعات و/یا امنیت و عملیات شبکه برعهده دارند و یا اشخاصی که مسوول برنامه امنیتی کلی سازمان و تدوین خطی‌مشی امنیتی هستند، شامل مدیران ارشد و یا دیگر مدیران و کاربران غیرفنی نیز می‌باشند.

این استاندارد مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جنبه‌های معماری امنیت شبکه، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

استاندارد ISO/IEC 18028-3 مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جزئی دروازه‌های امنیتی، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

استاندارد ISO/IEC 18028-4 مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جزیی امنیت دسترسی راه دور، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

استاندارد ISO/IEC 18028-5 مربوط به تمام کارکنانی است که در طرح‌ریزی، طراحی و پیاده‌سازی جزیی VPNها، درگیر هستند (مانند مدیران، مجریان، مهندسین شبکه و مسوولان امنیتی شبکه).

فناوری اطلاعات – فنون امنیتی – امنیت شبکه فناوری اطلاعات –

قسمت ۲: معماری امنیتی شبکه

۱- هدف و دامنه کاربرد

هدف از تدوین این استاندارد ارائه یک معماری امنیتی شبکه را به‌منظور فراهم‌سازی یک امنیت انتها به انتهای شبکه است. این معماری می‌تواند در انواع مختلف شبکه که در آن امنیت انتها به انتها حایز اهمیت است و مستقل از فناوری استفاده شده در شبکه، به‌کار گرفته شود. هدف این قسمت از مجموعه استانداردهای ملی ایران ISO/IEC 18028، ارائه یک زیربنائی برای تدوین استانداردهای مفصل‌تر در زمینه امنیت انتها به انتهای شبکه می‌باشد.

۲- مراجع الزامی

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

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

استفاده از مراجع زیر برای این استاندارد الزامی است

- استاندارد ISO 7498-2:1989، سامانه‌های پردازش اطلاعات – اتصال متقابل سامانه‌های باز – مدل مرجع پایه‌ای قسمت ۲: معماری امنیتی
- توصیه‌نامه CCITT X.800 (1991)، معماری امنیتی برای سامانه‌های باز – اتصال متقابل برای کاربردهای CCITT.

۳- اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر که در استاندارد ISO 7498-2 (1989) و توصیه‌نامه CCIT Rec X.800 تعریف شده‌اند، بکار می‌رود:

۳-۱-

کنترل دسترسی[1]

پیش‌گیری از استفاده غیرمجاز از یک منبع، شامل پیش‌گیری از استفاده از یک منبع به یک حالت نامعتبر.

[1] Access control

۳-۲-

احراز اصالت منشاء داده[1]

تأیید این‌که منبع داده دریافتی همان است که ادعا می‌شود.

۳-۳-

احراز اصالت موجودیت همتا[2]

تأیید این‌که یک موجودیت همتا در یک پیوند، همان است که ادعا می‌شود.

۳-۴-

در دسترس بودن[3]

ویژگی دسترسی‌پذیری و قابل استفاده بودن به محض تقاضا توسط یک موجودیت مجاز.

۳-۵-

محرمانگی[4]

این ویژگی که اطلاعات، دردسترس افراد، موجودیت‌ها و فرایندهای غیر مجاز قرار داده نمی‌شود و افشاء نمی‌گردد.

۳-۶-

یکپارچگی داده[5]

این ویژگی که داده به روش غیرمجاز تغییر داده نشده و یا تخریب نگردیده است.

۳-۷-

انکارناپذیری با اثبات منشاء[6]

سرویسی امنیتی که اثباتی از هویت منشاء داده را در اختیار دریافت کننده داده قرار می‌دهد.

---

[1] Data origin authentication
[2] Peer-entity authentication
[3] Availability
[4] Confidentiality
[5] Data integrity
[6] Non-repudiation with proof of origin

یادآوری۱ این سرویس، از هر تلاش فرستنده در رابطه با انکار نادرست ارسال داده یا محتوای آن، جلوگیری می‌کند.

یادآوری۲ از ISO 7498-2 |CCITT Rec. X.800 اقتباس شده‌است.

۳-۸-

انکارناپذیری با اثبات تحویل[1]

سرویس امنیتی که در آن تحویل داده برای فرستنده داده، اثبات می‌شود.

یادآوری۱ این سرویس امنیتی، از هر تلاش متعاقب دریافت‌کننده در رابطه با انکار نادرست دریافت داده یا محتوی آن جلوگیری می‌کند.

یادآوری۲ اقتباس شده از ISO 7498-2 |CCITT Rec. X.800 .

۳-۹-

حریم خصوصی[2]

حق افراد در زمینه کنترل و تاثیرگذاری روی نوع اطلاعاتی که ممکن است در مورد آن‌ها جمع‌آوری و ذخیره شود و این‌که اطلاعات توسط چه کسانی جمع‌آوری و ذخیره شده و برای چه کسانی آشکار می‌شود.

[1] Non-repudiation with proof of delivery
[2] Privacy

۴- کوته‌واژگان

واژه اختصاری	عبارت کامل انگلیسی	عبارت کامل فارسی
ASP	Application Service Provider	ارائه‌دهنده سرویس کاربرد
ATM	Asynchronous Transfer Mode	حالت انتقال غیرهمزمان
DHCP	Dynamic Host Configuration Protocol	پروتکل پیکربندی پویای میزبان
DS-3	Digital Signal level 3	سیگنال دیجیتال سطح ۳
IPsec	IP Security protocol	پروتکل امنیتی IP
MD5	Message digest Version 5	چکیده پیغام نسخه ۵
OAM&P	Operations Administration Maintenance & Provisioning	عملیات، اداره، نگهداری و تدارکات
OSI	Open Systems Interconnection	اتصالات متقابل سامانه‌های باز
PSTN	Public Switched Telephone Network	شبکه تلفن سوئیچینگ عمومی
PVC	Permanent Virtual Circuit	مدار مجازی دائمی
SHA-1	Secure Hash Algorithm	الگوریتم درهم‌سازی امن
SIP	Session Initiation Protocol	پروتکل آغاز نشست
SMTP	Simple Mail Transfer Protocol	پروتکل ساده انتقال پستی
SONET	Synchronous Optical Network	شبکه نوری همزمان
SS7	Signalling System #7	سامانه سیگنالینگ شماره هفت
SSL	Secure Socket Layer (encryption and authentication protocol)	لایه سوکت امن (پروتکل رمزگزاری و احراز اصالت)
TLS	Transport Layer Security(encryption and authentication protocol)	امنیت لایه انتقال (پروتکل رمزگزاری و احراز اصالت)
VLAN	Virtual Local Area Network	شبکه محلی مجازی

۵- معماری مرجع برای امنیت شبکه

معماری مرجع برای چالش‌های امنیتی جهانی ارائه‌دهندگان سرویس، بنگاه‌های اقتصادی و مصرف‌کنندگان، ایجاد گردیده است و در مورد شبکه‌های صوت، داده و نیز همگرای بی‌سیم، نوری، باسیم قابل اعمال است. در متن این مدرک، واژه مرجع به همراه واژه معماری، برای بیان این مطلب به کار می‌رود که مشخصه بیان شده، مثالی از یک معماری امنیتی سطح بالا می‌باشد که می‌تواند به‌عنوان یک مبنا در طراحی راه‌حل‌های امنیتی مفصل‌تر برای شبکه‌های متنوع مورداستفاده قرار گیرد. این معماری مرجع، به مفاهیم امنیتی مرتبط با امر مدیریت، کنترل و استفاده از زیرساخت، سرویس‌ها و برنامه‌های کاربردی شبکه اشاره دارد. معماری مرجع یک نمای انتهابه‌انتها، بالا به پائین و جامع را از امنیت شبکه ارائه می‌نماید و در مورد اجزا، سرویس‌ها و برنامه‌های کاربردی، به‌منظور پیش‌بینی، کشف و تصحیح آسیب‌پذیری‌های امنیتی قابل اعمال است.

معماری مرجع، مجموعه پیچیده خصیصه‌های امنیتی انتها به انتهای شبکه را به‌طور منطقی به مؤلفه‌های معماری مجزا تقسیم می‌کند. این جداسازی، امکان ارائه یک رویکرد نظام‌مند به امنیت انتهابه‌انتها در شبکه را فراهم می‌کند که می‌تواند در برنامه‌ریزی برای راه‌حل‌های امنیتی ونیز ارزیابی و شناسائی امنیت شبکه‌های موجود، مورداستفاده قرار گیرد.

معماری مرجع به نیازهای امنیتی شبکه که پوشش‌دهنده سوالات اساسی زیر می‌باشد، پاسخ‌می‌دهد:

۱. از چه نوعی ازاطلاعات لازم است، حفاظت شود؟
۲. یک مخاطره امنیتی چیست و برای مدیریت مخاطرات امنیتی، چه نوعی از حفاظت موردنیاز است؟
۳. چه‌نوعی از فعالیت‌های مجزای شبکه، لازم است تحت حفاظت قرار گیرند؟
۴. کدام نوع از تجهیزات و تسهیلات مجزای شبکه لازم است حفاظت شوند؟

لازم است ارزیابی مخاطرات امنیتی، به‌منظور اولویت‌بندی نیازهای حفاظتی و همچنین کمک نمودن به تعیین اقدامات امنیتی مناسب برای معماری شبکه، انجام پذیرد.

این سوالات توسط سه مولفه معماری‌گونه ابعاد امنیتی، سطوح امنیتی و لایه‌های امنیتی مورد بحث قرار می‌گیرند.

اصول و قواعد تشریح‌شده توسط معماری مرجع چندوجهی، مستقل از فناوری به‌کار گرفته شده در شبکه یا موقعیت در پشته پروتکل، در گستره متنوعی از شبکه‌ها، قابل اعمال می‌باشد.

۶- ابعاد امنیتی

به‌طور معمول در یک فرایند مدیریت مخاطره، اقدامات امنیتی مناسبی به‌منظور مدیریت یا کاهش مخاطرات ارزیابی شده، شناسایی می‌شود. یک بعد امنیتی، بیانگر مجموعه‌ای از اقدامات امنیتی است که به‌منظور پیاده‌سازی جنبه‌های خاصی از امنیت شبکه، به‌کار می‌روند. مفهوم ابعاد امنیتی، محدود به شبکه‌ها نمی‌باشد، بلکه در مورد برنامه‌های کاربردی و اطلاعات کاربر انتهایی نیز قابل بکارگیری است. علاوه بر این،

ابعاد امنیتی در مورد ارائه‌دهندگان سرویس یا بنگاه‌های اقتصادی که به ارائه سرویس‌های امنیتی به مشتریان خود می‌پردازند نیز قابل اعمال است. ابعاد امنیتی عبارتند از:

۱. کنترل دسترسی
۲. احراز اصالت
۳. انکارناپذیری
۴. محرمانگی داده
۵. امنیت جریان ارتباطات
۶. یکپارچگی داده
۷. در دسترس بودن
۸. حریم خصوصی

ابعاد امنیتی که به‌طور صحیح طراحی و پیاده سازی شده‌اند از خطی‌مشی امنیتی که برای یک شبکه خاص تعریف می‌شود، پشتیبانی می‌کنند و قواعد تنظیم شده توسط مدیریت امنیت را تسهیل می‌نمایند.

۶-۱- بعد امنیتی کنترل دسترسی

بعد امنیتی کنترل دسترسی، مجوزهای لازم را برای استفاده از منابع شبکه تخصیص می‌دهد. کنترل دسترسی اطمینان می‌دهد که فقط کارکنان یا وسایل مجاز، اجازه دسترسی به عناصر، اطلاعات ذخیره شده، جریان‌های اطلاعات، سرویس‌ها و برنامه‌های کاربردی شبکه را دارند. برای مثال، کنترل دسترسی مبتنی بر نقش[1]، سطوح مختلفی را فراهم می‌کند تا تضمین نماید که فقط افراد و دستگاه‌هایی می‌توانند به عناصر اطلاعات ذخیره شده و جریان‌های اطلاعاتی از شبکه دسترسی داشته باشند و عملیاتی را روی آن‌ها انجام دهند که برای این موارد مجاز باشند.

۶-۲- بعد امنیتی احراز اصالت

بعد امنیتی احراز اصالت، برای تایید شناسه‌ها یا دیگر خصیصه‌های مجوزدهی موجودیت‌های ارتباطی به‌کار می‌رود. احراز اصالت، موجب حصول اطمینان از اعتبار شناسه‌های ادعاشده موجودیت‌های شرکت‌کننده در ارتباطات (به‌عنوان مثال شخص، وسیله، سرویس یا برنامه‌های کاربردی) می‌شود و تضمین می‌کند که موجودیت‌ها، تلاش برای تکرار پاسخ‌های جعلی یا غیر مجاز از ارتباط پیشین را ندارند. در روش‌های احراز اصالتی که از شیوه‌های مبتنی بر شناسه کاربر، زوج کلمه عبور، احراز اصالت دوعاملی[2] (مثل نشانه) استفاده می‌کنند، زیست‌سنجی[3] از جمله روش‌های پرکاربرد می‌باشد.

[1] Role-Based Access Control , RBAC
[2] Two-factor
[3] Biometric

۶-۳- بعد امنیتی انکارناپذیری

بعد امنیتی انکارناپذیری با ارائه اثباتی قابل دسترس در مورد فعالیت‌های مختلف مربوط به شبکه (نظیر اثبات وظیفه، قصد یا التزام، منشاء داده، مالکیت، اثبات استفاده از منبع)، روش‌هایی فنی را به‌منظور ممانعت از انکار یک شخص یا موجودیت از انجام یک عمل مشخص انجام شده بر روی داده، فراهم می‌کند. این بعد به حصول اطمینان از در دسترس بودن یک مدرک که می‌تواند به‌عنوان یک اثبات فنی به شخص ثالث ارائه شود تا ثابت شود که یک نوع رویداد یا عمل به وقوع پیوسته است، کمک می‌کند. توجه کنید که انکار ناپذیری که توسط ابزار فنی فراهم گشته است، الزاماً به یک نتیجه‌گیری قانونی منتهی نمی‌شود. از روش‌های رمزنگاری اغلب برای اثبات انکارناپذیری استفاده می‌شود.

۶-۴- بعد امنیتی محرمانگی داده

بعد امنیتی محرمانگی داده، از افشای غیرمجاز داده حفاظت می‌کند. رمزگزاری، روشی است که اغلب برای حصول اطمینان از محرمانگی داده، استفاده می‌شود. فهرست‌های کنترل دسترسی و مجوزهای فایل، روش‌هایی می‌باشند که به حفظ محرمانگی داده کمک می‌کنند.

۶-۵- بعد امنیتی جریان ارتباطات

بعد امنیتی جریان ارتباطات اطمینان می‌دهد که اطلاعات تنها بین نقاط انتهایی مجاز، جریان دارد (اطلاعات در هنگام عبور از میان این نقاط، منحرف و یا شنود نمی‌شود). سازوکارهای امنیتی بعد امنیتی جریان اطلاعات، تحریف و تغییر را حفاظت نمی‌کنند. این عمل یکی از کارکردهای یکپارچگی داده می‌باشد. تونل‌های MPLS [1]، VLANها وVPNها[2] فناوری‌هایی می‌باشند که می‌توانند امنیت جریان اطلاعات را فراهم کنند.

۶-۶- بعد امنیتی یکپارچگی داده

بعد امنیتی یکپارچگی داده، موجب حصول اطمینان از درستی یا یکپارچگی داده می‌شود، (بدین معنی‌که داده تنها توسط فرآیندها و روش‌های مجاز یا فعالیت‌های افراد و وسایل مجاز پردازش می‌شود). با اعمال این بعد، داده در برابر تغییرات غیرمجاز، حذف، ایجاد و تکرار حفاظت می‌شود و علاوه برآن، نشانه‌ای از فعالیت‌های غیر مجاز را در اختیار قرار می‌دهد. معمولاً از روش‌های کد تصدیق اصالت پیغام درهم سازی شده[3] (به‌عنوان مثال SHA-1, MD5) برای حصول اطمینان از یکپارچگی داده، استفاده می‌شود.

[1] Multi Protocol Label Switching,
[2] Virtual Private Networks
[3] Hashed Message Authentication Code, HMAC

۶-۷- بعد امنیتی در دسترس بودن

بعد امنیتی در دسترس بودن اطمینان می‌دهد که برای دسترسی مجاز به عناصر، اطلاعات ذخیره شده، جریان‌های داده، سرویس‌ها و برنامه‌های کاربردی شبکه، هیچ انسدادی به دلیل رویدادهایی که شبکه را تحت‌تأثیر قرار می‌دهند، وجود نخواهد داشت. راه‌حل‌های بازیابی پس از وقوع حادثه، در این دسته قرار می‌گیرند.

۶-۸- بعد امنیتی حریم خصوصی

بعد امنیتی حریم خصوصی به حفاظت از هر نوع اطلاعاتی (مربوط به یک شخص، ارتباطات یا هر نوع داده – شامل سرآیندهای بسته‌ای – هر نوع فعالیت انجام شده توسط این شخص) می‌پردازد که ممکن است از مشاهده فعالیت‌های شبکه استنتاج شود. نمونه‌هایی از این نوع اطلاعات عبارتند از تارنما[1]هایی که یک کاربر از آن‌ها دیدن نموده است، موقعیت جغرافیائی یک کاربر، آدرس‌های IP و اسامی DNS [2] دستگاه‌ها در یک شبکه ارائه‌دهنده سرویس. ترجمه آدرس‌های شبکه (NAT)[3] و پروکسی‌های برنامه کاربردی، نمونه‌هایی از شیوه‌هایی می‌باشند که می‌توانند جهت حفاظت از حریم خصوصی به‌کار گرفته شوند. برحسب قوانین و مقررات مربوط به حریم خصوصی ملی و حفاظت داده‌ها، بعد امنیتی حریم خصوصی بایستی ساختار حفاظتی و کنترل‌های مناسبی جهت جمع‌آوری، پردازش و انتشار اطلاعات شخصی ارائه نماید.

۷- لایه‌های امنیتی

به‌منظور ارائه یک راه‌حل امنیتی انتهابه‌انتها، ابعاد امنیتی توصیف شده در بخش قبل باید به سلسله مراتبی از تجهیزات شبکه و گروه‌های تسهیلاتی که از آن‌ها به‌عنوان لایه‌های امنیتی یاد می‌شود، اعمال شود. معماری مرجع، سه لایه امنیتی- لایه امنیتی زیرساخت، لایه امنیتی سرویس و لایه امنیتی کاربرد را تعریف می‌کند. این لایه‌های امنیتی جهت تدارک راه‌حل‌های مبتنی بر شبکه، بر روی هم بنا می‌شوند.

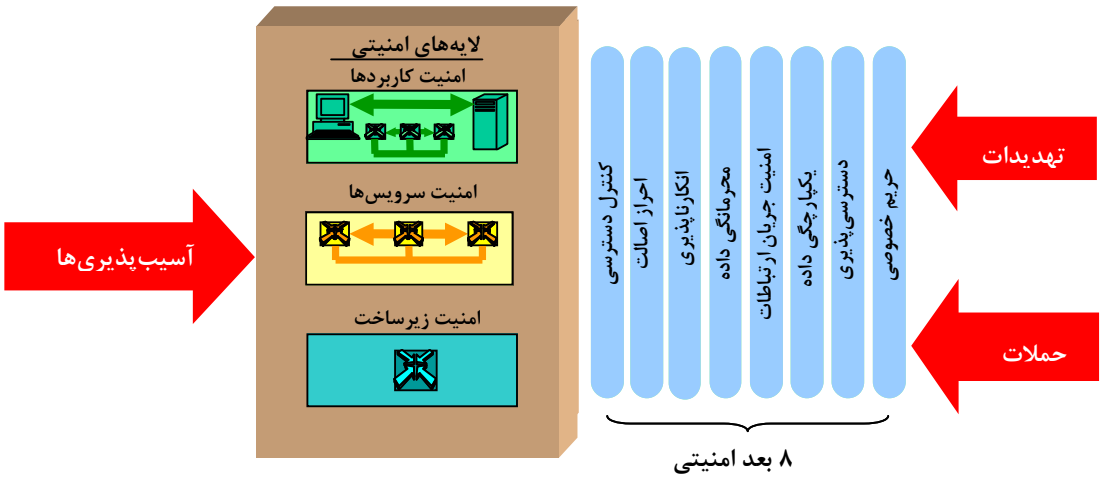
لایه‌های امنیتی، مجموعه‌هایی از توانمندسازها[4] برای راه‌حل‌های امن شبکه می‌باشند. لایه امنیتی زیرساخت، لایه امنیتی سرویس را و لایه امنیتی سرویس، لایه امنیتی کاربرد را فعال می‌کند. معماری مرجع، بیانگر این واقعیت است که هر لایه، دارای آسیب‌پذیری‌های امنیتی متفاوتی است و مناسب‌ترین روش مقابله با حملات بالقوه را برای یک لایه امنیتی خاص پیشنهاد می‌کند. تصمیم‌گیری در مورد این‌که آیا لایه‌های بالایی باید فرض کنند که عملکرد امنیتی لایه زیرین همان‌گونه است که انتظار می‌رود، می‌باشد یا اینکه بایستی فرایندهایی جهت آشکارسازی و کشف خرابی‌ها در لایه‌های زیرین به‌کار گرفته شوند، در هنگام پیاده‌سازی یک شبکه صورت می‌گیرد.

---

[1] website
[2] Domain Name Sevice
[3] Network Address Translation
[4] Enablers

لازم به ذکر است که مفهوم لایه‌های امنیتی (همان‌گونه که در بالا تعریف شدند) متفاوت ازمفهوم لایه‌های OSI می‌باشند.

لایه‌های امنیتی با ارائه یک نمای ترتیبی از امنیت شبکه، بخش‌هائی از محصولات و راه‌حل‌ها که برقراری امنیت در آن باید در نظر گرفته شود، را مشخص می‌کنند. به‌عنوان‌مثال، آسیب‌پذیری‌های امنیتی، نخست برای لایه امنیتی زیرساخت، سپس برای لایه امنیتی سرویس و در نهایت برای لایه امنیتی کاربرد مورد بررسی قرار می‌گیرند. ابعاد امنیتی، نواحی‌ای از هر لایه امنیتی که لازم است به‌منظور برقراری امنیت مورد توجه قرار گیرند، را مشخص می‌کنند. شکل ۱ چگونگی اعمال سازوکارهای موجود در هر بعد امنیتی به لایه‌های امنیتی را به‌منظور کاهش آسیب‌پذیری‌های موجود در هر لایه و در نتیجه کاهش حملات امنیتی نشان می‌دهد.



شکل ۱- اعمال ابعاد امنیتی به لایه‌های امنیتی

۷-۱- لایه امنیتی زیرساخت

لایه امنیتی زیرساخت، از تسهیلات انتقال شبکه و نیز بخش‌ها و عناصر مجزای شبکه تشکیل شده است که توسط سازوکارهای پیاده‌سازی شده برای ابعاد امنیتی، حفاظت می‌شوند. لایه امنیتی زیرساخت، نمایانگر بلوک‌های اساسی سازنده شبکه‌ها، سرویس‌ها و کاربردهای آن‌ها می‌باشد. چند نمونه از مولفه‌های متعلق به لایه امنیتی زیرساخت شامل مسیریاب‌های مجزا، سوده[1]ها و سرویس‌دهندگان و نیز پیوند[2]های ارتباطی بین مسیریاب‌های مجزا، سوده‌ها و سرویس‌دهندگان می‌باشد.

[1] Switch
[2] Link

۷-۲- لایه امنیتی سرویس‌ها

لایه امنیتی سرویس‌ها بیانگر امنیت سرویس‌هایی است که ارائه‌دهندگان سرویس، برای مشتریان خود فراهم می‌کنند. این سرویس‌ها از سرویس‌های انتقال پایه و اتصال به توانمندسازهای سرویس‌ها مانند سرویس‌هایی که برای ایجاد دسترسی به اینترنت ضروری می‌باشند (به عنوان مثال سرویس‌های احراز اصالت، مجوزدهی و سرویس‌های پاسخگوئی، سرویس‌های پیکربندی پویای میزبان[۱]، سرویس‌های پویای نام حوزه و غیره) تا سرویس‌های ارزش افزوده نظیر سرویس رایگان تلفنی، QoS[۲]، VPN، سرویس‌های مکان‌یابی[۳]، پیام‌رسانی آنی[۴] و غیره را در برمی‌گیرند.

لایه امنیت سرویس جهت حفاظت از ارائه‌دهندگان و مشتریان آن‌ها که هر دو، جزء اهداف بالقوه تهدیدات امنیتی می‌باشند، مورداستفاده قرارمی‌گیرد. به‌عنوان‌مثال ممکن است مهاجمان سعی در ناتوان کردن ارائه‌دهندگان سرویس برای ارائه سرویس داشته باشند و یا تلاش کنند سرویس مربوط به یک مشتری خاص ارائه‌دهنده سرویس (نظیر یک شرکت) را مختل کنند.

۷-۳- لایه امنیتی کاربردها

لایه امنیتی کاربردها، بر امنیت برنامه‌های کاربردی مبتنی بر شبکه که توسط مشتریان ارایه‌دهندگان سرویس قابل دسترسی می‌باشند، متمرکز است. این برنامه‌های کاربردی به وسیله سرویس‌های شبکه، فعال می‌شوند و شامل انتقال فایل اصلی (مانندFTP [۵])، برنامه‌های کاربردی جستجوگر وب، برنامه‌های کاربردی زیربنایی نظیر فهرست‌یاری، پیام‌رسانی صوتی و نامه الکترونیکی مبتنی بر شبکه و نیز برنامه‌های کاربردی گران قیمت همچون مدیریت روابط مشتری، تجارت سیّار/الکترونیک ، آموزش مبتنی بر شبکه، تعامل تصویری و غیره می‌باشند. برنامه‌های کاربردی مبتنی بر شبکه ممکن است توسط ASPهای شخص ثالث، ارایه‌دهندگان سرویسی که به‌صورت ارایه‌دهندگان سرویس برنامه کاربردی فعالیت می‌نمایند و یا بنگاه‌های اقتصادی که مراکز داده خود را در اختیار آن‌ها قرار داده‌اند (یا اجاره داده‌اند)، ارایه شوند. در این لایه، چهار هدف بالقوه برای حملات امنیتی وجود دارد. این اهداف عبارتند از:

۱. کاربر برنامه کاربردی
۲. ارائه‌دهنده برنامه کاربردی
۳. میان‌افزار تهیه‌شده توسط یکپارچه‌کننده‌های شخص ثالث (مانند سرویس‌های میزبان وب)
۴. ارایه‌دهنده سرویس

---

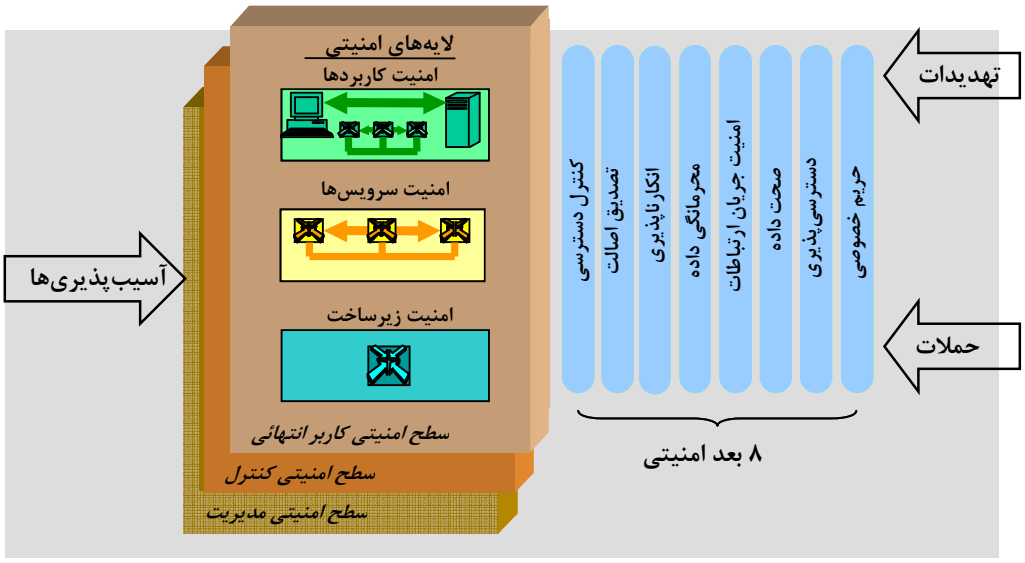
[1] Dynamic Host Configuration Sevices , DHCS
[2] Quality of Service
[3] Location Services
[4] Instant messaging
[5] File Transport Protocol

۸- سطوح امنیتی

یک سطح امنیتی، یک نوع مشخص از فعالیت شبکه است که توسط ساز وکارهایی که برای ابعاد امنیتی پیاده‌سازی شده‌اند، حفاظت می‌شود. این معماری مرجع، سه سطح امنیتی را برای نمایش سه نوع فعالیت حفاظت‌شده که در شبکه به‌وقوع می‌پیوندد، تعریف می‌کند. این سطوح امنیتی عبارتند از: ۱) سطح امنیتی مدیریت، ۲) سطح امنیتی کنترل، ۳) سطح امنیتی کاربر انتهایی. این سطوح امنیتی به ترتیب به نیازهای خاص امنیتی مرتبط با فعالیت‌های مدیریتی، فعالیت‌های سیگنالینگ یا کنترل شبکه و فعالیت‌های کاربر انتهایی اشاره می‌کنند.

شبکه‌ها بایستی به‌گونه‌ای طراحی شوند که تا حد ممکن رویدادهائی که در یک سطح امنیتی رخ می‌دهند به‌نحوی مناسب از سایر سطوح امنیتی مجزا نگاه داشته شوند. برای مثال انبوهی از جداول جستجوی DNS در سطح امنیتی کاربر که توسط تقاضاهای کاربر انتهایی آغاز شده‌اند، نبایستی واسط OAM&P در سطح امنیتی مدیریت که اجازه تصحیح مشکل به مدیر اجرایی می‌دهد را مسدود کند.

شکل۲ معماری مرجع را همراه با سطوح امنیتی نشان می‌دهد. هر نوع از فعالیت‌های شبکه‌ای توصیف‌شده، دارای نیازهای امنیتی خاص خود می‌باشد. مفهوم سطح امنیتی این امکان را فراهم می‌کند که مسایل امنیتی خاص مرتبط با آن فعالیت‌ها را از همدیگر تمیز دهیم و به‌طور مستقل از هم به آن‌ها بپردازیم. برای مثال، یک سرویسVoIP[1] را در لایه امنیتی سرویس‌ها نظر بگیرید. امن‌سازی مدیریت سرویس VoIP (نظیر تدارکات برای کاربران) بایستی مستقل از امن‌سازی کنترل سرویس VoIP (مثل، پروتکل‌هایی از قبیل SIP) و نیز مستقل از امن‌سازی داده در حال انتقال کاربر انتهایی توسط سرویس (مانند صدای کاربر) باشد.



شکل ۲- سطوح امنیتی منعکس‌کننده انواع مختلف فعالیت‌های شبکه هستند.

[1] Voice Over IP

۸-۱- سطح امنیتی مدیریت

سطح امنیتی مدیریت به حفاظت از کارکردهای OAM&P عناصر شبکه، تسهیلات انتقال، سامانه‌های پشتیبان اداری (اعم از سامانه‌های پشتیبان عملیات، سامانه‌های پشتیبان تجاری، سامانه‌های امور مشتریان و غیره) و مراکز داده مربوط می‌شود. سطح امنیتی مدیریت از عملیات «خطا، ظرفیت، مدیریت‌های اجرایی، تدارکات و امنیت» (FCAPS) [1] پشتیبانی می‌کند. قابل ذکر است که شبکه‌ای که ترافیک مربوط به این فعالیت‌ها را حمل می‌کند، با توجه به ترافیک کاربر متعلق به ارایه‌دهنده سرویس ممکن است «درباند»[2] یا «برون‌باند»[3] باشد.

۸-۲- سطح امنیتی کنترل

سطح امنیتی کنترل در رابطه با حفاظت از فعالیت‌هایی است که تحویل موثر اطلاعات، سرویس‌ها و برنامه‌های کاربردی را در طول شبکه‌ها، میسر می‌کنند. این امر به‌طور معمول شامل ارتباطات ماشین به ماشین اطلاعات است که این امکان را فراهم می‌کند که ماشین‌ها (به عنوان مثال سوده‌ها و مسیریاب‌ها) تعیین کنند چگونه به بهترین صورت، مسیریابی یا سودهی ترافیک را در طول شبکه انتقال درگیر انجام دهند. به این اطلاعات گاهی اوقات اطلاعات کنترلی یا سیگنالینگ اطلاق می‌شود. شبکه‌ای که این‌گونه پیغام‌ها را انتقال می‌دهد نسبت به ترافیک کاربر متعلق به ارایه دهنده سرویس، ممکن است «درباند» یا «برون‌باند» باشد. برای مثال، شبکه‌های IP، اطلاعات کنترلی خود را به‌صورت «درباند» منتقل می‌کنند، درحالی‌که شبکه‌های PSTN، اطلاعات سیگنالینگ خود را در یک شبکه خارجی جداگانه و به‌صورت «برون باند» منتقل می‌کنند (شبکه SS7). پروتکل‌های مسیریابی، DNS، SIP، SS7، Megaco/H.246، H.248 و غیره نمونه‌هایی از این نوع ترافیک می‌باشند.

۸-۳- سطح امنیتی کاربر انتهایی

سطح امنیتی کاربر انتهایی به امنیت دسترسی و استفاده از شبکه ارایه‌دهنده سرویس توسط مشتریان اشاره می‌کند. همچنین این سطح مرتبط با حفاظت از جریان‌های واقعی داده کاربر انتهایی است. کاربران انتهایی ممکن است از شبکه‌ای که تنها اتصال را برقرار می‌کند، استفاده کنند و ممکن است آن‌ها را به‌منظور استفاده از سرویس‌های ارزش‌افزوده از قبیل شبکه‌های VPN یا دسترسی به برنامه‌های کاربردی مبتنی بر شبکه به‌کار برند.

۹- تهدیدات امنیتی

معماری مرجع، یک طرح و مجموعه‌ای از اصول و قوانین را تعریف می‌کند که یک ساختار امنیتی را برای راه‌حل امنیتی انتهابه‌انتها توصیف می‌نمایند. این معماری، عناوین امنیتی که نیاز است به‌منظور

[1] Fault, Capacity, Administration, Provisioning and Security
[2] In-Band
[3] Out of Band

پیش‌گیری از تهدیدات عمدی و غیرعمدی مورد بررسی قرار گیرند را مشخص می‌کند. تهدیداتی که در ادامه به آنها اشاره می‌شود، در CCIT Rec. X. 800 (1991) l ISO 7498-2:1989، شرح داده شده‌اند.

- تخریب اطلاعات و/یا سایر منابع
- تحریف یا تغییر اطلاعات
- سرقت، حذف، یا از دست رفتن اطلاعات و/یا سایر منابع
- افشای اطلاعات
- وقفه در سرویس و انسداد سرویس‌دهی

فصل مشترک و محل تقاطع هر لایه امنیتی با هر سطح امنیتی بیانگر یک نمای امنیتی است که در آن ابعاد امنیتی جهت مقابله با تهدیدات اعمال می‌شوند. جدول ۱، یک نگاشت از ابعاد امنیتی به تهدیدات امنیتی را ارایه می‌کند. این نگاشت برای هر نمای امنیتی یکسان است.

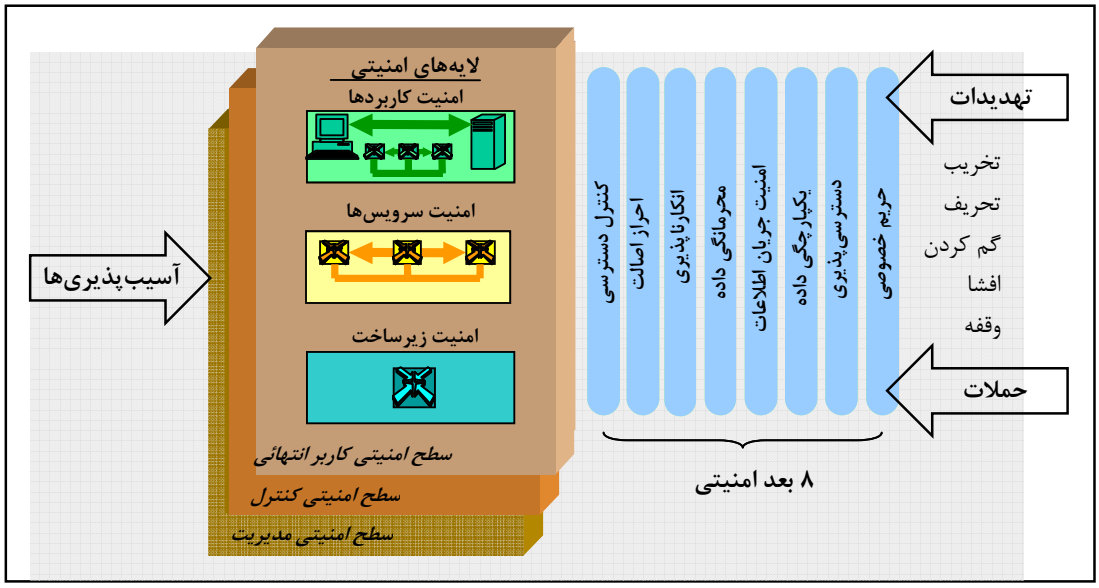
حرف "Y" که در خانه مربوط به تقاطع سطرها و ستون‌های جدول قرار دارد، مقابله با یک تهدید به‌خصوص امنیتی توسط بعد امنیتی متناظر آن را نشان می‌دهد.

جدول ۱- نگاشت ابعاد امنیتی به تهدیدات امنیتی

ابعاد امنیتی	تهدیدات امنیتی				
	تخریب اطلاعات یا سایر منابع	تحریف یا تغییر اطلاعات	سرقت، حذف یا از دست رفتن اطلاعات و سایر منابع	افشای اطلاعات	وقفه در سرویس و انسداد سرویس‌دهی
کنترل دسترسی	Y	Y	Y	Y	
احراز اصالت			Y	Y	
انکارناپذیری	Y	Y	Y	Y	Y
محرمانگی داده			Y	Y	
امنیت جریان ارتباطات			Y	Y	
یکپارچگی داده	Y	Y			
در دسترس بودن	Y				Y
حریم خصوصی				Y	

شکل ۳، معماری مرجع را با عناصر معماری نمایش می‌دهد و تهدیدات امنیتی توصیف‌شده فوق را نشان می‌دهد. این شکل، مفهوم حفاظت از شبکه توسط ابعاد امنیتی موجود در هر سطح امنیتی از هر لایه امنیتی را به‌منظور ارایه یک راه‌حل امنیتی فراگیر نشان می‌دهد. لازم به ذکر است که بسته به نیازهای امنیتی یک

شبکه، ممکن است نیاز به پیاده‌سازی تمامی عناصر معماری نباشد (به معنای داشتن مجموعه کاملی از ابعاد امنیتی، لایه‌های امنیتی و سطوح امنیتی).



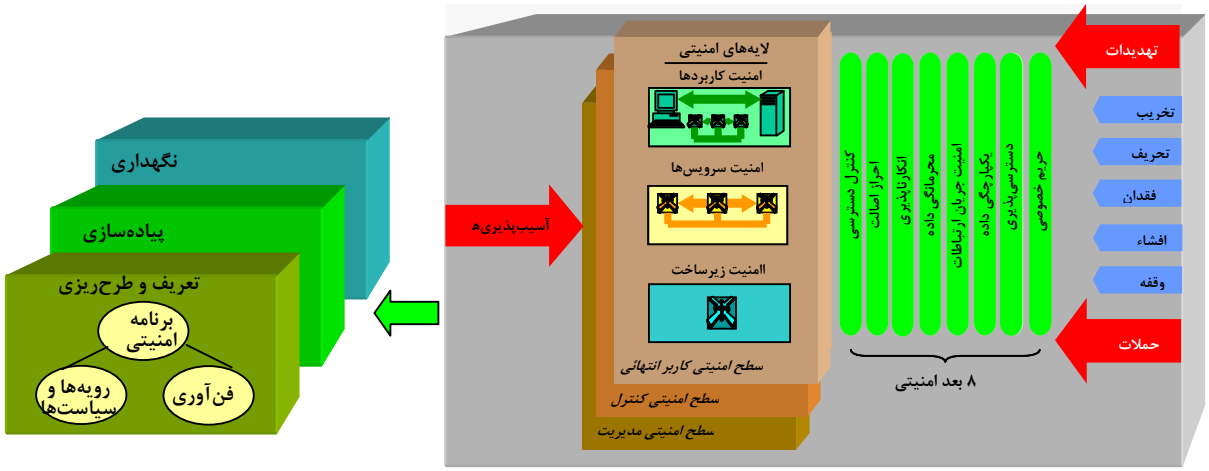
شکل ۳- معماری مرجع برای امنیت انتهابه‌انتهای شبکه

۱۰- توصیف اهداف به‌دست آمده با به کارگیری ابعاد امنیتی به لایه‌های امنیتی

معماری مرجع را می‌توان برای تمام وجوه و مراحل یک برنامه امنیتی به صورتی‌که در شکل ۴ نشان داده شده است، به‌کار برد. چنانچه در شکل ۴ دیده می‌شود، یک برنامه امنیتی علاوه بر فناوری، شامل خطی‌مشی‌ها و رویه‌هایی است که در طول عمر خود از سه مرحله زیر عبور می‌کنند: ۱) مرحله تعریف و طرح‌ریزی، ۲) مرحله پیاده‌سازی، ۳) مرحله نگهداری. این معماری مرجع همراه با راهنمایی‌های ارایه شده در استاندارد ISO/IEC 13335 قابل بکارگیری برای خطی‌مشی‌ها و رویه‌های امنیتی و نیز فناوری‌های به‌کار رفته، در تمام سه مرحله برنامه امنیتی است.

بر اساس نیازهای کسب وکار معماری شبکه، تعاریف خطی‌مشی‌ها، پاسخ به رخدادها و طرح‌های بازیابی تعیین می‌شوند. در این فرایند، معماری مرجع می‌تواند در زمینه تدوین تعاریف خطی‌مشی امنیتی جامع، طرح‌های پاسخ به رخداد و بازیابی و معماری‌های فناوری، راهنمایی‌هایی را با احتساب هر بعد امنیتی در هر لایه و هر سطح امنیتی در طول مرحله تعریف و طرح‌ریزی ارایه کند. معماری مرجع می‌تواند به‌عنوان مبنایی به‌منظور ارزیابی امنیتی استفاده شود تا بررسی شود چگونه پیاده‌سازی یک برنامه امنیتی، ابعاد، لایه‌ها و سطوح امنیتی را با گسترش خطی‌مشی‌ها، رویه‌ها و فناوری تعیین می‌کند. زمانی‌که یک برنامه امنیتی اعمال شد، لازم است این برنامه به‌منظور حفظ جریان تغییر مداوم محیط امنیتی، پشتیبانی شود. معماری مرجع می‌تواند در مدیریت سیاست‌ها و رویه‌های امنیتی، طرح‌های پاسخ به رخدادها و بازیابی و نیز معماری‌های

فناوری، جهت حصول اطمینان از اینکه تغییرات برنامه امنیتی به هر بعد امنیتی در هر سطح و لایه امنیتی اشاره دارد، کمک کند.



شکل ۴- اعمال معماری امنیتی مرجع به برنامه‌های امنیتی

علاوه بر این، معماری مرجع را می‌توان برای هر نوع شبکه، در هر سطح از پشته پروتکل به‌کار برد. به‌عنوان مثال، در یک شبکه IP که در لایه سه پشته پروتکل قرار می‌گیرد، لایه امنیتی زیرساخت به تک‌تک مسیریاب‌ها، پیوندهای ارتباطی نقطه‌به‌نقطه بین مسیریاب‌ها (مثل SONET، ATM PVCs و غیره) و سکوهای[1] سرویس‌دهندگان که برای پشتیبانی از سرویس‌های مورد نیاز شبکه IP مورد استفاده قرار می‌گیرند، اشاره می‌کند. لایه امنیتی سرویس به سرویس پایه‌ای IP (اتصال اینترنتی)، سرویس‌های پشتیبان IP (مانند AAA[2]، DNS[3]، DHCP و غیره) و سرویس‌های با ارزش‌افزوده پیشرفته که توسط ارایه‌دهنده سرویس فراهم می‌شود (مانند VOIP، QoS، VPNها و .غیره) می‌پردازد. سرانجام لایه امنیتی کاربرد به امنیت کاربردهای کاربران که باید از طریق شبکه IP فراهم شود، اشاره می‌کند (مانند پست الکترونیکی و غیره).

همین‌طور، برای یک شبکه ATM که در لایه دو پشته پروتکل قرار دارد، لایه امنیتی زیرساخت به تک‌تک سوده‌ها و پیوندهای ارتباطی نقطه‌به‌نقطه بین سوده‌ها (تجهیزات انتقال مانند DS-3) اشاره می‌کند. لایه امنیتی سرویس به کلاس‌های متفاوت انتقال فراهم‌شده توسط سرویس ATM (نرخ بیت ثابت[4]، نرخ بیت متغیر - بلادرنگ[5]، نرخ بیت متغیر - غیر بلادرنگ[6]، نرخ بیت در دسترس[7] و نرخ بیت نامشخص[8]) اشاره

[1] Platform
[2] Authentication, Authorization, Accounting
[3] Domain Name Service
[4] Constant Bit Rate
[5] Variable Bit Rate- Real Time
[6] Variable Bit Rate-non- Real Time
[7] Available Bit Rate
[8] Unspecified Bit Rate

می‌کند. در نهایت، لایه امنیتی کاربرد اشاره به کاربردهایی دارد که کاربر با استفاده از شبکه ATM، به آنها دسترسی می‌یابد نظیر کاربرد تعامل تصویری.

شکل ۵ معماری مرجع را به شکل جدول ارایه می‌کند و یک رویکرد منظم را برای امن کردن یک شبکه نشان می‌دهد. همان‌گونه که در این شکل دیده می‌شود، تقاطع یک لایه امنیتی با یک سطح امنیتی، یک چشم‌انداز و نمای یکتا برای لحاظ کردن هشت بعد امنیتی را نمایش می‌دهد. هر یک از ۹ ماژول، هشت بعد امنیتی که به یک لایه امنیتی خاص در یک سطح امنیتی خاص اعمال می‌شوند را ترکیب می‌کنند.

باید توجه شود که ابعاد امنیتی ماژول‌های متفاوت ممکن است دارای اهداف متفاوت بوده و در نتیجه شامل مجموعه‌هایی متفاوت از اقدامات امنیتی باشند. شکل جدول‌گونه ارایه‌شده، راه‌کار مناسبی برای توصیف اهداف ابعاد امنیتی هر ماژول ارایه می‌دهد. باید یادآوری شود که مفهوم حفاظت که در جداول زیر به‌کار گرفته شده است، شامل ایجاد مکانیزم‌هایی برای کشف اینکه در چه مکان‌هایی مکانیزم‌های کنترلی از کار می‌افتند و حصول اطمینان از اینکه رویدادها به‌منظور عکس‌العمل مناسب گزارش می‌شوند و یا دستگاه‌ها/فرایندهایی در محل نتایج ناشی از خرابی را برطرف می‌کنند، است.

	لایه امنیتی زیرساخت	لایه امنیتی سرویس	لایه امنیتی کاربرد
سطح امنیتی مدیریت	ماژول ۱	ماژول ۴	ماژول ۷
سطح امنیتی کنترل	ماژول ۲	ماژول ۵	ماژول ۸
سطح امنیتی کاربر انتهایی	ماژول ۳	ماژول ۶	ماژول ۹

جریان ارتباطات	کنترل دسترسی
یکپارچگی داده	احراز اصالت
در دسترس بودن	انکارناپذیری
حریم خصوصی	محرمانگی داده

شکل ۵- معماری مرجع به شکل جدول‌گونه

۱۰-۱- لایه امنیتی زیرساخت

امن‌سازی سطح امنیتی مدیریت لایه امنیتی زیرساخت در رابطه با امن‌سازی عملیات، مدیریت، نگهداری، تدارکات و پیکربندی تک‌تک عناصر شبکه، پیوندهای ارتباطی و سکوهای[1] سرویس‌دهندگان که شبکه را تشکیل می‌دهند، می‌باشد. به‌عنوان مثالی از مدیریت زیرساخت که لازم است امن شود، می‌توان به پیکربندی تک‌تک مسیریاب‌ها یا سوده‌ها توسط کارکنان عملیات شبکه اشاره نمود.

[1] Platform

جدول ۲ اهداف اعمال ابعاد امنیتی به لایه امنیتی زیر ساخت سطح امنیتی مدیریت را شرح می‌دهد.

جدول ۲- اعمال ابعاد امنیتی به لایه امنیتی زیرساخت، سطح امنیتی مدیریت

ماژول ۱: لایه امنیتی زیرساخت، سطح امنیتی مدیریت	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه فقط کارکنان یا وسایل مجاز (به‌عنوان مثال وسایلی که توسط پروتکل SNMP مدیریت می‌شوند) می‌توانند بر روی وسیله شبکه یا پیوند ارتباطی، فعالیت‌های مدیریتی و اجرایی انجام دهند و یا برای انجام این فعالیت‌ها تلاش نمایند. این مساله، به هر دو صورت مدیریت مستقیم وسیله از طریق یک درگاه دستی و مدیریت راه دور وسیله، قابل اعمال است.
احراز اصالت	شناسه شخص و یا وسیله‌ای که روی وسیله شبکه‌ای یا پیوند ارتباطی، فعالیت مدیریتی و اجرایی انجام می‌دهد را تصدیق می‌کند. فنون احراز اصالت ممکن است به‌عنوان بخشی از فرایند کنترل دسترسی مورد نیاز باشند.
انکارناپذیری	یک سابقه ثبت‌شده جهت شناسایی شخص یا وسیله انجام‌دهنده فعالیت مدیریتی یا اجرایی روی وسیله شبکه‌ای یا پیوند ارتباطی و همچنین شناسایی فعالیت انجام‌گرفته، فراهم می‌کند. این سابقه می‌تواند به‌عنوان اثباتی از هویت آغازگر فعالیت مدیریتی یا اجرایی استفاده شود.
محرمانگی داده	اطلاعات پیکربندی یک وسیله شبکه‌ای یا پیوند ارتباطی را از دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. این بعد امنیتی به اطلاعات پیکربندی مستقر در وسیله شبکه یا پیوند ارتباطی و اطلاعات پیکربندی در حال ارسال به وسیله شبکه‌ای یا پیوند ارتباطی و همچنین به اطلاعات پیکربندی پشتیبان[1] که به‌صورت برون‌خط ذخیره شده‌اند، اعمال می‌گردد. اطلاعات مدیریتی احراز اصالت (مثل کلمه عبور و شناسه‌های مدیر اجرایی) را از دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. فنون استفاده‌شده در کنترل دسترسی ممکن است در فراهم آوردن محرمانگی داده نیز مشارکت داشته باشند.

[1] Backup Information Configuration

امنیت جریان ارتباطات	حصول اطمینان از اینکه در مورد مدیریت از راه‌دور یک وسیله شبکه‌ای و یا پیوند ارتباطی، اطلاعات مدیریتی فقط بین ایستگاه‌های مدیریت از راه دور و دستگاه‌ها و پیوندهای ارتباطی که مدیریت می‌شوند، جریان می‌یابند. اطلاعات مدیریتی در جریان بین این نقاط انتهایی منحرف نشده و یا شنود نمی‌شود. نوع یکسانی از این ملاحظات در مورد اطلاعات مدیریت اجرائی احراز اصالت (مثل شناسه‌ها و کلمه‌های عبور مدیر اجرایی) اعمال می‌شود.
یکپارچگی داده	اطلاعات پیکربندی وسایل شبکه‌ای و پیوندهای ارتباطی را در مقابل تغییرات غیرمجاز حفاظت می‌کند. این بعد امنیتی حفاظتی به اطلاعات پیکربندی مستقر در وسیله شبکه‌ای یا پیوند ارتباطی و همچنین اطلاعات پیکربندی که در حال عبور و یا ذخیره‌شده در سامانه‌های برون خط هستند، اعمال می‌گردد. نوع یکسانی از این ملاحظات در مورد اطلاعات مدیریت اجرایی احراز اصالت (مثل شناسه‌ها و کلمه‌های عبور مدیر اجرایی) اعمال می‌شود.
دسترسی‌پذیری	حصول اطمینان از اینکه توانایی مدیریت وسیله شبکه‌ای یا پیوند ارتباطی توسط کارکنان و یا وسایل مجاز، قابل انکار نیست. این امر شامل حفاظت در مقابل حملات فعال مانند DoS و همچنین حفاظت در مقابل حملات غیرفعال مانند تغییر یا حذف اطلاعات مدیریت اجرائی احراز اصالت (مثل شناسه‌ها و کلمه‌های عبور مدیر اجرایی) است.
حریم خصوصی	حصول اطمینان از اینکه اطلاعاتی که می‌تواند برای شناسایی وسیله شبکه‌ای یا یک پیوند ارتباطی استفاده شود، در دسترس کارکنان و یا وسایل غیرمجاز نیست. مثال‌هایی از این‌گونه اطلاعات شامل آدرس IP یک وسیله شبکه‌ای یا اسم حوزه DNS است. به‌عنوان مثال توانایی شناسایی وسایل شبکه یا پیوندهای ارتباطی، اطلاعات هدف‌یابی را برای حمله‌کنندگان فراهم می‌سازد. حصول اطمینان از اینکه اطلاعات شخصی در شبکه، بر طبق قوانین و مقررات محلی حفاظت از داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

امن‌سازی سطح امنیتی کنترل لایه امنیتی زیرساخت شامل امن‌سازی اطلاعات کنترلی یا سیگنالینگ مستقر در عناصر شبکه و سکوهای سرویس‌دهندگانی که شبکه را تشکیل می‌دهند و نیز امن‌سازی دریافت و انتقال اطلاعات کنترلی یا سیگنالینگ توسط عناصر شبکه و سکوهای سرویس‌دهندگان می‌باشد. به‌عنوان مثال، جداول سودهی که در سوده‌های شبکه قرار دارند، لازم است از مداخله و افشای غیرمجاز محافظت

شوند. در مثالی دیگر، مسیریاب‌ها لازم است از/یا دربرابر دریافت و انتشار جداول به‌روزرسانی مدیریت مسیریابی جعلی یا پاسخ دادن به درخواست‌های جعلی مسیریابی که از مسیریاب‌های تغییر چهره داده‌شده، ارسال می‌شوند، محافظت شوند. جدول ۳، اهداف اعمال ابعاد امنیتی در لایه امنیتی زیرساخت سطح امنیتی کنترل را توصیف می‌کند.

جدول ۳- اعمال ابعاد امنیتی به لایه امنیتی زیرساخت، سطح امنیتی کنترل

ماژول ۲: لایه امنیتی زیرساخت، سطح امنیتی کنترل	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه فقط کارکنان و وسایل مجاز می‌توانند به اطلاعات کنترلی مستقر در یک وسیله شبکه، (مانند جدول مسیریابی)، یا یک ذخیره‌گاه[1] برون خط دسترسی یابند یا برای دسترسی به آن تلاش کنند. حصول اطمینان از اینکه وسیله شبکه پیام‌های اطلاعات کنترلی را فقط از وسیله شبکه مجاز قبول می‌کند (مانند به‌روزرآمدی مسیریابی).
احراز اصالت	هویت شخص و یا وسیله مشاهده‌کننده یا تغییردهنده اطلاعات کنترلی مستقر در یک وسیله شبکه را تصدیق می‌کند. هویت وسیله فرستنده اطلاعات کنترلی به وسیله شبکه را تصدیق می‌کند. فنون احراز اصالت ممکن است به‌عنوان بخشی از فرایند کنترل دسترسی مورد نیاز باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که امکان شناسایی هر شخص یا وسیله شبکه‌ای که اطلاعات یک وسیله شبکه‌ای را مشاهده یا اطلاعات کنترلی‌اش را تغییر داده است و همچنین عملی که انجام گرفته است را ممکن می‌سازد. این سابقه می‌تواند به عنوان اثباتی از دسترسی یا تغییر دادن اطلاعات کنترلی استفاده شود. یک سابقه‌ای را فراهم می‌سازد که با استفاده از آن امکان شناسایی وسیله فرستنده پیغام‌های کنترلی به یک وسیله شبکه و همچنین شناسایی عملی که انجام گرفته است، فراهم می‌شود. این سابقه می‌تواند به عنوان اثباتی از این که پیغام کنترلی از این وسیله نشأت گرفته است، استفاده شود.
محرمانگی داده	اطلاعات کنترلی مستقر در یک وسیله شبکه‌ای و یا یک ذخیره‌گاه برون خط را در مقابل دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. فنون مورد استفاده در کنترل دسترسی، ممکن است در فراهم‌سازی محرمانگی داده برای اطلاعات کنترلی مستقر در یک وسیله شبکه‌ای مشارکت کنند. اطلاعات کنترلی فرستاده‌شده به یک وسیله شبکه‌ای را در حال انتقال در شبکه، از دسترسی غیرمجاز یا مشاهده غیرمجاز حفاظت می‌کند.

[1] Storage

امنیت جریان ارتباطات	حصول اطمینان از اینکه اطلاعات کنترلی در حال انتقال در شبکه (نظیر جداول مسیریابی) فقط بین منبع فرستنده اطلاعات و هدف در نظر گرفته‌شده آن جریان می‌یابند. اطلاعات کنترلی در جریان انتقال بین دو نقطه انتهایی انحراف مسیر نیافته و یا شنود نمی‌شوند.
یکپارچگی داده	اطلاعات کنترلی مستقر در وسایل شبکه‌ای، در حال انتقال در شبکه، یا ذخیره‌شده برون خط را در مقابل تغییرات غیرمجاز حفاظت می‌کند.
دسترسی‌پذیری	حصول اطمینان از اینکه وسایل شبکه‌ای همیشه برای دریافت اطلاعات کنترلی از منابع مجاز در دسترس هستند. این خود شامل حفاظت در مقابل حملات ناخواسته مانند حملات DoS و رخدادهای اتفاقی (به عنوان مثال تغییر مسیر) می‌باشد.
حریم خصوصی	حصول اطمینان از اینکه اطلاعاتی که می‌توانند برای شناسایی وسیله شبکه یا یک پیوند ارتباطی استفاده شود در دسترس کارکنان یا وسایل غیرمجاز نیست. مثال‌هایی از این‌گونه اطلاعات شامل آدرس IP یا اسم حوزه DNS است. برای مثال توانایی شناسایی وسایل شبکه‌ای یا پیوندهای ارتباطی، اطلاعات هدف‌یابی را برای حمله‌کنندگان فراهم می‌سازد. حصول اطمینان از اینکه اطلاعات شخصی در طول شبکه بر طبق قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

امن‌سازی سطح امنیتی کاربر انتهایی لایه امنیتی زیرساخت، امن‌سازی داده و صدای کاربر در حالی‌که در عناصر شبکه قرار دارد و یا از میان آن‌ها انتقال می‌یابد و همچنین هنگامی‌که در طول پیوندهای ارتباطی انتقال می‌یابد، را شامل می‌شود. حفاظت از داده کاربر که مستقر در سکوهای سرویس‌دهندگان است و همچنین حفاظت از داده کاربر که در حال انتقال در طول عناصر شبکه یا در عرض پیوندهای ارتباطی می‌باشد، در مقابل شنود غیرمجاز، حایز اهمیت است. جدول ۴ اهداف اعمال ابعاد امنیتی به لایه امنیتی زیرساخت و سطح امنیتی کاربر انتهایی را توصیف می‌کند.

جدول ۴- اعمال ابعاد امنیتی به لایه امنیتی زیرساخت، سطح امنیتی کاربر انتهایی

ماژول ۳: لایه امنیتی زیرساخت، سطح امنیتی کاربر انتهایی	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه فقط کارکنان و وسایل مجاز می‌توانند به اطلاعات کاربر انتهایی که در حال گذر از یک عنصر شبکه یا یک پیوند ارتباطی، یا ذخیره‌شده در یک ذخیره‌گاه برون خط است، دسترسی یابند یا برای دسترسی به آن تلاش کنند.
احراز اصالت	هویت شخص و یا وسیله‌ای که می‌خواهد به اطلاعات کاربر انتهایی که در حال گذر از یک عنصر شبکه یا یک پیوند ارتباطی یا مستقر در یک ذخیره‌گاه برون خط است، دسترسی پیدا کند، را تصدیق می‌کند. فنون احراز اصالت ممکن است به‌عنوان بخشی از فرایند کنترل دسترسی مورد نیاز باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که هر شخص یا وسیله شبکه‌ای که می‌خواهد به اطلاعات کاربر انتهایی که در حال گذر از یک عنصر شبکه یا یک پیوند ارتباطی یا مستقر در وسایل برون خط است، دسترسی پیدا کند، و همچنین عملی که انجام شده است را شناسایی می‌کند. این سابقه می‌تواند به عنوان اثباتی از دسترسی به اطلاعات کاربر انتهایی استفاده شود.
محرمانگی داده	اطلاعات کاربر انتهایی که در حال گذر از یک عنصر شبکه یا یک پیوند ارتباطی است یا در وسایل برون خط مستقر شده است، را در مقابل دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. فنون مورد استفاده در تعیین کنترل دسترسی ممکن است به فراهم‌سازی محرمانگی داده برای اطلاعات کاربر انتهایی، کمک کنند.
امنیت جریان ارتباطات	حصول اطمینان از اینکه اطلاعات کاربر انتهایی که در حال گذر از یک عنصر شبکه یا یک پیوند ارتباطی است، در جریان انتقال بدون دسترسی مجاز (مانند استراق‌سمع‌های قانونی) انحراف مسیر نیافته و یا شنود نمی‌شود.
یکپارچگی داده	اطلاعات کاربر انتهایی که در حال گذر از یک عنصر شبکه یا یک پیوند ارتباطی است، یا در یک وسیله برون خط، مستقر شده است را در مقابل تغییرات غیرمجاز حفاظت می‌کند.

دسترسی‌پذیری	حصول اطمینان از اینکه دسترسی به اطلاعات کاربر انتهایی که در وسایل مستقر است، توسط کارکنان مجاز (شامل کاربران انتهایی) و وسایل غیرقابل انسداد است. این امر شامل حفاظت در برابر حملات فعال مانند حملات DoS و حملات غیرفعال مانند تغییر یا حذف اطلاعات احراز اصالت (نظیر شناسه‌ها و کلمه‌های عبور کاربران، شناسه‌ها و کلمات عبور مدیران اجرایی) می‌باشد.
حریم خصوصی	حصول اطمینان از اینکه عناصر شبکه‌ای، اطلاعات مربوط به فعالیت‌های شبکه‌ای کاربر انتهایی(مانند محل جغرافیایی کاربر، تارنماهایی که مراجعه کرده است و غیره) را در اختیار کارکنان یا وسایل غیرمجاز قرار نمی‌دهند. حصول اطمینان از اینکه اطلاعات شخصی در طول شبکه بر طبق قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش شده و انتشار می‌یابند.

۱۰-۲- لایه امنیتی سرویس‌ها

امن کردن لایه امنیتی سرویس‌ها به‌دلیل این‌که ممکن است سرویس‌ها جهت تامین نیازهای مشتریان بر روی یکدیگر بنا گردند، بسیار پیچیده است. به‌عنوان مثال، یک ارایه‌دهنده سرویس به‌منظور ارایه یک سرویس VoIP، ابتدا می‌بایست سرویس IP پایه همراه با سرویس فعال‌کننده موردنیاز همچنین سرویس‌هایی نظیر AAA، DHCP، DNS و غیره را ایجاد نماید. همچنین ممکن است، ارایه‌دهنده سرویس برای تامین سرویس QoS مشتریان و نیازهای امنیتی سرویس VoIP نیاز به توسعه یک سرویس VPN داشته باشد. از این‌رو، هنگام آدرس‌دهی به امنیت کلی یک سرویس، لازم است در ابتدا آن سرویس به سرویس‌های مرکبی که در ایجاد آن به‌کار رفته‌اند، تجزیه گردد.

امن کردن سطح امنیتی مدیریت لایه امنیتی سرویس‌ها، به منزله امن کردن کارکردهای OAM&P و همچنین امن کردن پیکربندی سرویس‌های شبکه می‌باشد. مثالی از مدیریت سرویس‌هایی که می‌بایست امن گردد، فراهم کردن یک سرویس کاربر انتهایی خاص برای کاربران مجاز توسط کارکنان عملیات شبکه می‌باشد. جدول ۵ اهداف اعمال ابعاد امنیتی به لایه امنیتی سرویس و سطح امنیتی مدیریت را توصیف می‌کند.

جدول ۵- اعمال ابعاد امنیتی به لایه امنیتی سرویس، سطح امنیتی مدیریت

ماژول ۴: لایه امنیتی سرویس، سطح امنیتی مدیریت	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه فقط کارکنان و وسایل مجاز می‌توانند فعالیت‌های مدیریتی و اجرایی سرویس شبکه‌ای/تحت شبکه (مانند تدارک دیدن سرویس برای کاربران) را انجام داده یا برای انجام آن‌ها تلاش کنند.
احراز اصالت	هویت شخص و یا وسیله تلاش‌کننده برای انجام فعالیت‌های مدیریتی و اجرایی سرویس شبکه‌ای را تصدیق می‌کند. فنون احراز اصالت ممکن است به‌عنوان بخشی از فرایند کنترل دسترسی مورد نیاز باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که هر شخص یا وسیله شبکه‌ای که اقدام به انجام فعالیت‌های مدیریتی و اجرایی سرویس شبکه‌ای کند را شناسایی می‌کند. این سابقه می‌تواند به عنوان اثباتی باشد مبنی بر اینکه شخص یا وسیله شبکه‌ای اقدام به انجام فعالیت مدیریتی و اجرایی کرده است.
محرمانگی داده	اطلاعات پیکربندی و مدیریتی سرویس شبکه‌ای (برای مثال تنظیمات قابل بارگیری IPsec مشتری برای سرویس VPN) را در برابر دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. این بعد امنیتی به اطلاعات مدیریتی و پیکربندی مستقر در وسایل شبکه، در حال انتقال در شبکه، یا ذخیره‌شده برون خط، اعمال می‌شود. این بعد امنیتی، اطلاعات پیکربندی و مدیریتی سرویس شبکه‌ای (مثل شناسه‌ها و کلمات عبور کاربر، شناسه‌ها و کلمات عبور مدیر اجرائی) را از دسترسی یا مشاهده غیرمجاز حفاظت می‌کند.
امنیت جریان ارتباطات	حصول اطمینان از اینکه در حالت مدیریت از راه‌دور یک سرویس شبکه‌ای، اطلاعات مدیریتی و اجرایی فقط بین ایستگاه مدیریت از راه دور و وسایل که به عنوان بخشی از سرویس شبکه‌ای مدیریت می‌شوند، جریان می‌یابد. اطلاعات مدیریتی و اجرائی در جریان این انتقال بین نقاط انتهائی انحراف مسیر نیافته و یا شنود نمی‌شوند. نوع یکسانی از این ملاحظات قابل اعمال به اطلاعات احراز اصالت برای سرویس شبکه‌ای (مثل شناسه‌ها و کلمات عبور کاربر، شناسه‌ها و کلمات عبور مدیر اجرائی) می‌باشد.

یکپارچگی داده	اطلاعات مدیریتی و اجرایی سرویس‌های شبکه‌ای را در مقابل تغییرات غیرمجاز حفاظت می‌کند. این بعد امنیتی به اطلاعات مدیریتی و اجرایی موجود در وسایل شبکه، در حال انتقال در شبکه، و یا ذخیره‌شده در سامانه‌های برون خط اعمال می‌گردد. نوع یکسانی از این ملاحظات قابل اعمال به اطلاعات احراز اصالت برای سرویس شبکه‌ای (مثل شناسه‌ها و کلمات عبور کاربر، شناسه‌ها و کلمات عبور مدیر اجرائی) است.
دسترسی‌پذیری	حصول اطمینان از اینکه توانایی مدیریت سرویس شبکه‌ای توسط کارکنان و وسایل مجاز، قابل انسداد نیست. این بعد امنیتی شامل حفاظت در مقابل حملات فعال مانند حملات DoS و حملات غیرفعال مانند تغییر و یا حذف اطلاعات مدیریتی احراز اصالت سرویس شبکه‌ای (نظیر شناسه‌ها و کلمات عبور مدیر اجرائی) است.
حریم خصوصی	حصول اطمینان از اینکه اطلاعاتی که می‌تواند برای شناسایی سامانه‌های مدیریتی یا اجرایی سرویس شبکه‌ای استفاده شود، در دسترس کارکنان یا وسایل غیرمجاز نیست. مثال‌هایی از این‌گونه اطلاعات، آدرس IP سامانه یا اسم حوزه DNS می‌باشد. به‌عنوان مثال توانایی سامانه‌های اجرائی سرویس شبکه‌ای، اطلاعات هدف‌یابی را برای حمله‌کنندگان فراهم می‌سازد. این بعد امنیتی، حصول اطمینان از اینکه اطلاعات شخصی در طول شبکه بر طبق قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

امن کردن سطح امنیتی کنترل لایه امنیتی سرویس‌ها شامل امن کردن اطلاعات کنترلی یا سیگنالینگ مورد استفاده توسط یک سرویس شبکه‌ای می‌باشد. به‌عنوان مثال موضوعات مرتبط با امن کردن پروتکل SIP که جهت راه‌اندازی و پشتیبانی نشست‌های VoIP به‌کار می‌رود، در این مقوله قرار می‌گیرد. جدول ۶ اهداف اعمال ابعاد امنیتی به سطح امنیتی کنترل لایه امنیتی سرویس‌ها را شرح می‌دهد.

جدول ۶- اعمال ابعاد امنیتی به لایه امنیتی سرویس، سطح امنیتی کنترل

ماژول۵: لایه امنیتی سرویس، سطح امنیتی کنترل	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه اطلاعات کنترلی دریافت‌شده توسط یک وسیله شبکه‌ای برای یک سرویس شبکه‌ای، قبل از پذیرش از یک منبع مجاز سرچشمه می‌گیرند (به‌عنوان مثال یک پیغام آغاز نشست VoIP از یک کاربر و یا وسیله مجاز سرچشمه می‌گیرد). به‌عنوان مثال حفاظت در برابر جعل هویت یک پیغام آغاز نشست VoIP، توسط یک وسیله غیرمجاز.
احراز اصالت	هویت منشاء فرستنده پیغام در بردارنده اطلاعات کنترلی مربوط به سرویس شبکه‌ای، که به وسایل شبکه‌ای شرکت‌کننده در سرویس، فرستاده شده است را تصدیق می‌کند. فنون احراز اصالت ممکن است به‌عنوان بخشی از فرایند کنترل دسترسی مورد نیاز باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که شناسه هر شخص یا وسیله شبکه‌ای منشاء ارسال پیغام‌های کنترلی سرویس شبکه‌ای، که توسط یک وسیله شبکه‌ای که در سرویس شبکه‌ای شرکت دارند، دریافت می‌شود و همچنین عملی که انجام گرفته است را شناسایی می‌کند. این سابقه می‌تواند به‌عنوان اثبات این‌که شخص یا وسیله مربوطه منشاء ارسال پیغام کنترلی سرویس شبکه‌ای است، استفاده شود.
محرمانگی داده	اطلاعات کنترلی سرویس شبکه‌ای مستقر در یک وسیله شبکه‌ای (مانند پایگاه داده‌های نشست‌های IPsec)، اطلاعات در حال انتقال در شبکه، یا ذخیره‌شده به‌صورت برون خط را در مقابل دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. فنون مورد استفاده در کنترل دسترسی ممکن است به فراهم‌سازی محرمانگی داده برای اطلاعات کنترلی سرویس شبکه‌ای مستقر در یک وسیله شبکه‌ای کمک کنند.
امنیت جریان ارتباطات	حصول اطمینان از اینکه اطلاعات کنترلی سرویس شبکه‌ای در حال انتقال در شبکه (نظیر پیغام‌های تبادل کلید IPsec) تنها بین منبع فرستنده اطلاعات کنترلی و هدف در نظر گرفته‌شده آن جریان می‌یابد. اطلاعات کنترلی سرویس شبکه‌ای در جریان این انتقال انحراف مسیر نیافته و یا شنود نمی‌شوند.

یکپارچگی داده	اطلاعات کنترلی سرویس شبکه‌ای مستقر در وسایل شبکه، در حال انتقال در شبکه، یا ذخیره‌شده برون خط را در برابر تغییرات غیرمجاز حفاظت می‌کند.
دسترسی‌پذیری	حصول اطمینان از اینکه وسایل شبکه مشارکت‌کننده در یک سرویس شبکه‌ای، همیشه برای دریافت اطلاعات کنترلی از منابع مجاز، در دسترس هستند. این امر شامل حفاظت در مقابل حملات فعال همچون حملات DoS می‌باشد.
حریم خصوصی	حصول اطمینان از اینکه اطلاعاتی که می‌تواند برای شناسایی وسیله شبکه‌ای یا یک پیوند ارتباطی استفاده‌شده در یک سرویس شبکه‌ای استفاده شود، در دسترس کارکنان یا وسایل غیرمجاز نیست. مثال‌هایی از این‌گونه اطلاعات شامل آدرس IP وسایل شبکه‌ای یا اسم حوزه DNS است. برای مثال توانایی شناسایی وسایل شبکه‌ای یا پیوندهای ارتباطی، اطلاعات هدف‌یابی را برای حمله‌کنندگان فراهم می‌سازد. حصول اطمینان از اینکه اطلاعات شخصی در طول شبکه بر طبق قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

امن کردن سطح امنیتی کاربر انتهایی لایه امنیتی سرویس شامل امن کردن داده‌ها و صوت کاربر در هنگام استفاده از یک سرویس شبکه می‌باشد. به عنوان مثال باید محرمانگی مکالمات یک کاربر، در یک سرویس VoIP حفاظت شود. همچنین یک DNS، باید از محرمانگی کاربران سرویس اطمینان حاصل کند. جدول ۷ اهداف اعمال ابعاد امنیتی به سطح امنیتی کاربر انتهایی لایه امنیتی سرویس‌ها را شرح می‌دهد.

جدول ۷- اعمال ابعاد امنیتی به لایه امنیتی سرویس، سطح امنیتی کاربر انتهایی

ماژول ۶: لایه امنیتی سرویس، سطح امنیتی کاربر انتهایی	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه فقط کارکنان و وسایل مجاز می‌توانند به سرویس شبکه‌ای دسترسی یابند یا برای دسترسی تلاش کنند.
احراز اصالت	هویت شخص و یا وسیله‌ای که می‌خواهد برای دسترسی و استفاده از سرویس شبکه‌ای تلاش کند را تصدیق می‌کند. فنون احراز اصالت ممکن است به‌عنوان بخشی از فرایند کنترل دسترسی مورد نیاز باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که هر کاربر یا وسیله‌ای که به یک سرویس شبکه‌ای دسترسی پیدا کرده و از آن استفاده کرده است، و نیز عملی که انجام شده است را شناسایی می‌کند. این سابقه می‌تواند به عنوان اثباتی از دسترسی و استفاده از سرویس شبکه‌ای از طرف کاربر انتهایی استفاده شود.

محرمانگی داده	اطلاعات کاربر انتهایی که در حال انتقال، پردازش یا ذخیره توسط سرویس شبکه‌ای است را در برابر دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. فنون مورد استفاده در کنترل دسترسی ممکن است به فراهم‌سازی محرمانگی داده برای اطلاعات کاربر انتهایی کمک کند.
امنیت جریان ارتباطات	حصول اطمینان از اینکه داده کاربر انتهایی که به‌وسیله یک سرویس شبکه‌ای، انتقال می‌یابد، پردازش و یا ذخیره می‌شود، در حین جریان بین این تقاط انتهایی، بدون دسترسی مجاز (مانند استراق‌سمع‌های قانونی)، انحراف مسیر نیافته و یا شنود نمی‌شود.
یکپارچگی داده	اطلاعات کاربر انتهایی که در حال انتقال، پردازش یا ذخیره توسط سرویس شبکه‌ای است را در برابر تغییرات غیرمجاز حفاظت می‌کند.
دسترسی‌پذیری	حصول اطمینان از اینکه دسترسی به سرویس‌های شبکه‌ای توسط کاربران یا وسایل مجاز، غیرقابل انسداد است. این امر شامل حفاظت در برابر حملات فعال مانند حملات DoS و حملات غیرفعال مانند تغییر یا حذف اطلاعات احراز اصالت کاربران انتهایی (مثلاً شناسه‌ها و کلمات عبور کاربران) است.
حریم خصوصی	حصول اطمینان از اینکه که سرویس شبکه‌ای، اطلاعات مربوط به فعالیت‌های شبکه‌ای کاربر انتهایی (به‌عنوان مثال برای یک سرویس VoIP، افرادی که با آن‌ها تماس گرفته شده است) را در اختیار کارکنان یا وسایل غیرمجاز قرار نمی‌دهد. حصول اطمینان از اینکه اطلاعات شخصی در طول شبکه بر طبق قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

۱۰-۳- لایه امنیتی کاربردها

امن کردن سطح امنیتی مدیریت لایه امنیتی کاربردها به منزله امن کردن کارکردهای مربوط به OAM&P و همچنین پیکربندی برنامه‌های کاربردی مبتنی بر شبکه می‌باشد. در زمینه کابردهای مربوط به پست الکترونیکی، مثالی از یک فعالیت مدیریتی که لازم است امن شود، تهیه و مدیریت صندوق پستی کاربران می‌باشد. جدول ۸ به شرح اهداف اعمال ابعاد امنیتی به سطح امنیتی مدیریت لایه امنیتی کاربردها می‌پردازد.

جدول ۸- اعمال ابعاد امنیتی به لایه امنیتی کاربرد، سطح امنیتی مدیریت

ماژول ۷: لایه امنیتی کاربرد، سطح امنیتی مدیریت	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه فقط کارکنان و وسایل مجاز می‌توانند فعالیت‌های مدیریتی و اجرایی کاربرد مبتنی بر شبکه (مانند مدیریت پست الکترونیکی کاربران برای یک کاربرد پست الکترونیکی) را انجام دهند یا برای انجام آن‌ها تلاش کنند.
احراز اصالت	هویت شخص و یا وسیله تلاش‌کننده به انجام فعالیت‌های مدیریتی و اجرایی مربوط به برنامه کاربرد مبتنی بر شبکه را تصدیق می‌کند. روش‌های احراز اصالت به‌عنوان بخشی از فرآیند کنترل دسترسی مورد نیاز می‌باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که هر شخص یا وسیله شبکه‌ای، که اقدام به انجام فعالیت‌های مدیریتی و اجرایی مربوط به یک برنامه کاربردی مبتنی بر شبکه کند و نیز عملی که انجام شده است را شناسایی می‌کند. این سابقه می‌تواند به عنوان اثباتی از اینکه شخص یا وسیله شبکه‌ای اقدام به انجام فعالیت مدیریتی و اجرایی کرده است، همراه با یک نشانی از شخص یا وسیله‌ای که آن عمل را انجام داده است، محسوب شود.
محرمانگی داده	از کلیه پرونده‌هایی که در ایجاد و اجرای برنامه‌های کاربردی مبتنی بر شبکه استفاده می‌شوند (مانند پرونده‌های منبع، پرونده‌های شیء، پرونده‌های اجرایی و پرونده‌های موقت و غیره) و نیز پرونده‌های پیکربندی برنامه کاربردی، در برابر دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. این بعد امنیتی به پرونده‌های برنامه‌های کاربردی که در وسایل شبکه‌ای مستقر می‌باشند، در شبکه در حال انتقال هستند و یا به‌صورت برون خط ذخیره شده‌اند، اعمال می‌شود. این بعد امنیتی، اطلاعات اجرایی یا مدیریتی برنامه‌های کاربردی مبتنی بر شبکه (به‌عنوان مثال، شناسه‌ها و کلمه‌های عبور کاربران، شناسه‌ها و کلمه‌های عبور مدیر اجرائی) را از دسترسی یا مشاهده غیرمجاز حفاظت می‌کند.
امنیت جریان ارتباطات	حصول اطمینان از اینکه در حالت مدیریت از راه دور یا مدیریت برنامه کاربردی مبتنی بر شبکه، اطلاعات مدیریتی و اجرایی فقط بین ایستگاه مدیریت از راه دور و دستگاه‌هایی که مرتبط با برنامه‌های کاربردی مبتنی بر شبکه هستند، جریان می‌یابد. اطلاعات مدیریتی و اجرایی در جریان این انتقال مابین دو نقطه انتهایی انحراف مسیر نیافته و یا شنود نمی‌شوند. نوع یکسانی از این ملاحظات در مورد اطلاعات مدیریتی و اجرایی برنامه‌های کاربردی مبتنی بر شبکه (مثل شناسه‌ها و کلمه‌های عبور کاربران، شناسه‌ها و کلمه‌های عبور مدیر اجرائی) به‌کار برده می‌شوند.

یکپارچگی داده	از تمام پرونده‌هایی که در ایجاد و اجرای برنامه‌های کاربردی مبتنی بر شبکه استفاده می‌شوند (مانند پرونده‌های منبع، پرونده‌های شیی، پرونده‌های اجرایی و پرونده‌های موقت و غیره) و نیز پرونده‌های پیکربندی برنامه کاربردی، دربرابر تغییرات غیرمجاز حفاظت می‌کند. این بعد امنیتی را می‌توان به پرونده‌های برنامه‌های کاربردی مستقر در وسایل شبکه‌ای، در حال انتقال در شبکه، یا ذخیره‌شده به‌صورت برون خط، اعمال کرد. نوع یکسانی از این ملاحظات در مورد اطلاعات مدیریتی و اجرایی برنامه‌های کاربردی مبتنی بر شبکه (مانند مثل شناسه‌ها و کلمه‌های عبور کاربر، شناسه‌ها و کلمات عبور مدیر اجرائی) به‌کار برده می‌شود.
دسترسی پذیری	حصول اطمینان از اینکه توانایی مدیریت کاربرد مبتنی بر شبکه، توسط کارکنان و وسایل مجاز قابل انسداد نیست. این امر شامل حفاظت در مقابل حملات فعال همچون حملات DoS و حملات غیرفعال مانند تغییر یا حذف اطلاعات مدیریتی احراز اصالت برنامه‌های کاربرد مبتنی بر شبکه (مانند شناسه‌ها و کلمه‌های عبور مدیر اجرائی) می‌باشد.
حریم خصوصی	حصول اطمینان از اینکه اطلاعاتی که می‌توانند برای شناسایی سامانه‌های مدیریتی یا اجرایی کاربرد مبتنی بر شبکه استفاده شوند، در دسترس کارکنان یا وسایل غیرمجاز نمی‌باشند. مثال‌هایی از این نوع اطلاعات شامل آدرس IP سامانه یا اسم حوزه DNS می‌باشد.به‌عنوان مثال توانایی شناسایی سامانه‌های اجرایی برنامه‌های کاربردی مبتنی بر شبکه، اطلاعات هدف‌یابی را برای مهاجمان فراهم می‌کند. حصول اطمینان از اینکه اطلاعات شخصی در طول شبکه به استناد قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

امن کردن سطح امنیتی کنترل لایه امنیتی کاربردها شامل امن کردن اطلاعات کنترلی یا سیگنالینگ استفاده‌شده توسط برنامه‌های کاربردی مبتنی بر شبکه می‌باشد. به‌طور معمول این نوع از اطلاعات منجر به این می‌شود که یک برنامه کاربردی عملی را در پاسخ به دریافت اطلاعات انجام دهد. به عنوان مثال موارد مربوط به امن کردن پروتکل‌های SMTP و POP که برای کنترل تحویل پست الکترونیکی به‌کار می‌روند در این‌جا بیان می‌شوند. جدول ۹ اهداف اعمال ابعاد امنیتی به سطح امنیتی کنترل لایه امنیتی کاربردها را شرح می‌دهد.

جدول ۹- اعمال ابعاد امنیتی به لایه امنیتی کاربرد، سطح امنیتی کنترل

ماژول ۸: لایه امنیتی کاربرد، سطح امنیتی کنترل	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه اطلاعات کنترلی برنامه کاربردی که توسط یک وسیله شبکه‌ای شرکت‌کننده در یک کاربرد مبتنی بر شبکه، دریافت شده است، قبل از پذیرش از یک منبع مجاز سرچشمه می‌گیرد (به‌عنوان مثال یک پیغام SMTP که درخواست انتقال یک پست الکترونیکی می‌کند). به‌عنوان مثال در برابر جعل هویت و سواستفاده از اصالت یک مشتری SMTP توسط یک وسیله غیرمجاز حفاظت می‌کند.
احراز اصالت	هویت منشاء فرستنده اطلاعات کنترلی کاربرد به وسایل شبکه‌ای شرکت‌کننده در کاربرد مبتنی بر شبکه را تصدیق می‌کند. فنون احراز اصالت به‌عنوان بخشی از فرآیند کنترل دسترسی مورد نیاز می‌باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که هر شخص یا وسیله شبکه‌ای فرستنده پیغام‌های کنترلی کاربرد که توسط وسیله شبکه‌ای شرکت‌کننده در کاربرد مبتنی بر شبکه دریافت می‌شوند و همچنین عملی که انجام گرفته است را شناسایی می‌کند. این سابقه می‌تواند به‌عنوان اثباتی از ارسال پیغام کنترلی مزبور توسط یک شخص یا وسیله مربوط، باشد.
محرمانگی داده	اطلاعات کنترلی کاربرد مستقر در یک وسیله شبکه‌ای (مانند پایگاه‌های داده نشست‌های SSL یا TLS)، در حال انتقال در شبکه یا ذخیره‌شده به‌صورت برون خط را در برابر دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. فنون مورد استفاده در کنترل دسترسی ممکن است به فراهم‌سازی محرمانگی داده برای اطلاعات کنترلی کاربرد مبتنی بر شبکه مستقر در یک وسیله شبکه‌ای کمک کنند.
امنیت جریان ارتباطات	حصول اطمینان از اینکه اطلاعات کنترلی کاربرد در حال انتقال در شبکه (نظیر پیغام‌های مذاکره TLS یا SSL) فقط بین منبع فرستنده اطلاعات کنترلی و هدف موردنظر آن جریان می‌یابند. اطلاعات کنترلی کاربرد مبتنی بر شبکه در جریان انتقال بین دو نقطه انتهایی انحراف و تغییر مسیر نیافته و یا شنود نمی‌شوند.
یکپارچگی داده	اطلاعات کنترلی کاربرد مبتنی بر شبکه مستقر در وسایل شبکه، در حال گذر از شبکه، یا ذخیره‌شده برون خط را در برابر تغییرات و حذف غیرمجاز حفاظت می‌کند.
دسترسی‌پذیری	حصول اطمینان از اینکه وسایل شبکه‌ای مشارکت‌کننده در یک کاربرد مبتنی بر شبکه همیشه برای دریافت اطلاعات کنترلی از منابع مجاز در دسترس هستند. این امر شامل حفاظت در مقابل حملات فعال مانند حملات DoS می‌باشد.

حریم خصوصی	حصول اطمینان از اینکه که اطلاعاتی که می‌تواند برای شناسایی وسایل شبکه‌ای یا یک پیوند ارتباطی شرکت‌کننده در یک کاربرد مبتنی بر شبکه استفاده شود، در دسترس کارکنان یا وسایل غیرمجاز نیست. مثال‌هایی از این نوع اطلاعات شامل آدرس IP وسیله شبکه یا اسم حوزه DNS است. به‌عنوان مثال توانایی شناسایی وسایل شبکه یا پیوندهای ارتباطی، اطلاعات هدف‌یابی را برای مهاجمان فراهم می‌سازد. این بعد امنیتی این اطمینان را فراهم می‌کند که اطلاعات شخصی در طول شبکه بر طبق قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

امن کردن سطح امنیتی کاربر انتهایی لایه امنیتی کاربرد، شامل امن کردن داده‌های کاربران است که در اختیار یک برنامه کاربردی قرار گرفته است. به‌عنوان مثال باید محرمانگی شماره کارت اعتباری یک کاربر، توسط یک برنامه کاربردی تجارت الکترونیک حفاظت شود. جدول ۱۰ به شریح اهداف اعمال ابعاد امنیتی به سطح امنیتی کاربر انتهایی لایه امنیتی کابردها می‌پردازد.

جدول ۱۰- اعمال ابعاد امنیتی به لایه امنیتی کاربرد، سطح امنیتی کاربر انتهایی

ماژول ۹: لایه امنیتی کاربرد، سطح امنیتی کاربر انتهایی	
بعد امنیتی	اهداف امنیتی
کنترل دسترسی	حصول اطمینان از اینکه فقط کاربران و وسایل مجاز، اجازه دسترسی یا تلاش برای دسترسی و استفاده از برنامه‌های کاربردی مبتنی بر شبکه را دارند.
احراز اصالت	هویت کاربر و یا وسیله‌ای که می‌خواهد برای دسترسی و استفاده از کاربرد مبتنی بر شبکه تلاش کند را تصدیق می‌کند. فنون احراز اصالت به‌عنوان بخشی از فرآیند کنترل دسترسی مورد نیاز می‌باشند.
انکارناپذیری	سابقه‌ای را فراهم می‌سازد که هر شخص یا وسیله شبکه‌ای که به یک کاربرد مبتنی بر شبکه دسترسی پیدا کرده و از آن استفاده کرده است و نیز عملی که انجام شده است را شناسایی می‌کند. این سابقه می‌تواند به‌عنوان اثباتی از دسترسی کاربر انتهایی یا وسیله به برنامه‌های کاربردی و استفاده از آن‌ها استفاده شود.
محرمانگی داده	اطلاعات کاربر انتهایی (مثل شماره کارت اعتباری کاربر) که در حال گذر، پردازش یا ذخیره توسط کاربرد مبتنی بر شبکه است را در برابر دسترسی یا مشاهده غیرمجاز حفاظت می‌کند. نوع یکسانی از این ملاحظات برای داده‌های کاربر که از طرف او به برنامه کاربردی مبتنی بر شبکه جریان می‌یابد، به‌کار برده می‌شود. فنون مورد استفاده در کنترل دسترسی ممکن است به فراهم‌سازی محرمانگی داده برای اطلاعات کاربر انتهایی کمک کنند.
امنیت جریان ارتباطات	حصول اطمینان از اینکه اطلاعات کاربر انتهایی که در حال انتقال، پردازش، یا ذخیره توسط کاربرد مبتنی بر شبکه است در جریان انتقال، بدون دسترسی مجاز (مانند استراق‌سمع

	مجاز و قانونی) انحراف مسیر نیافته و یا شنود نمی‌شوند. نوع یکسانی از این ملاحظات در مورد داده‌های کاربر که از طرف او به کاربرد مبتنی بر شبکه جریان می‌یابد، به‌کار برده می‌شود.
یکپارچگی داده	اطلاعات کاربر انتهایی که در حال انتقال، پردازش، یا ذخیره توسط کاربرد مبتنی بر شبکه است، را در مقابل تغییرات غیرمجاز حفاظت می‌کند. نوع یکسانی از این ملاحظات برای داده‌های کاربر که از طرف او به برنامه‌های کاربردی مبتنی بر شبکه در جریان می‌باشد، به‌کار برده می‌شود.
دسترسی‌پذیری	حصول اطمینان از اینکه دسترسی به کاربرد مبتنی بر شبکه توسط کاربران یا وسایل مجاز غیر قابل انسداد است. این امر شامل حفاظت در برابر حملات فعال مانند حملات DoS و حملات غیرفعال مانند تغییر یا حذف اطلاعات احراز اصالت کاربران انتهایی (به‌عنوان مثال شناسه‌ها و کلمه‌های عبور کاربران) است.
حریم خصوصی	حصول اطمینان از اینکه که برنامه‌های کاربردی مبتنی بر شبکه، اطلاعات مربوط به فعالیت‌های شبکه‌ای کاربر انتهایی و استفاده کاربر انتهایی از برنامه‌های کاربردی (نظیر تارنماهای مراجعه‌شده) را در اختیار کارکنان یا وسایل غیرمجاز قرار نمی‌دهد. به‌عنوان مثال این‌گونه اطلاعات فقط برای کارکنان مجری قانون مجاز به جستجو، افشا می‌شود. این بعد امنیتی این اطمینان را فراهم می‌کند که اطلاعات شخصی در طول شبکه بر طبق قوانین و مقررات محلی حفاظت داده، جمع‌آوری و پردازش می‌شوند و انتشار می‌یابند.

ICS: 35.040

صفحه : ۳۳