INSO
17641
1st. Edition
2013

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

استاندارد ملی ایران
۱۷۶۴۱
چاپ اول
۱۳۹۱

فناوری اطلاعات- فنون امنیتی- تصدیق پروتکل‌های رمزنگاشتی

Information technology - Security techniques - Verification of cryptographic protocols

ICS:35.040

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

« فناوری اطلاعات- فنون امنیتی- تصدیق پروتکل‌های رمزنگاشتی »

رئیس:	**سمت و/ یا نمایندگی**
صفایی، سپیده (کارشناس کامپیوتر)	کارشناس نرم‌افزار شرکت داده‌کاوان امن‌پرداز
دبیر:	
منافی، علیرضا (کارشناس ارشد کامپیوتر)	مدیر عامل شرکت امن‌افزار گستر شریف
اعضاء: (اسامی‌به ترتیب حروف الفبا)	
اخوان نیاکی، سید انوشیروان (کارشناس ارشد مدیریت فناوری اطلاعات)	مشاور مدیر عامل و مدیر مرکز مدیریت دانش و داده کاوی شرکت ایزایران
علی محمد ملایری، عصمت (کارشناس ارشد نرم‌افزار)	مدرس دانشگاه آزاد ملایر
مروجی، سجاد (کارشناس ارشد رایانه)	مدرس دانشگاه
مهدوی، سید علیرضا (کارشناس ارشد مدیریت فناوری اطلاعات)	مشاور شرکت داده‌پردازان آبشار
ولی،ناصر (کارشناس ارشد نرم‌افزار)	کارشناس فناوری اطلاعات کمیته امداد امام خمینی

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد«فناوری اطلاعات- فنون امنیتی- تصدیق پروتکل‌های رمزنگاشتی » که پیش نویس آن درکمیسیون‌های مربوط توسط شرکت امن افزار شریف تهیه و تدوین شده و در دویست و شصت و ششمین اجلاسیه کمیتهٔ ملی استانداردرایانه و فرآوری داده مورخ ۱۳۹۱/۱۲/۶ .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 همگامی‌و هماهنگی با تحولات و پیشرفت‌های 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.

منبع و مأخذی که برای تدوین این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 29128:2011 Information technology - Security techniques - Verification of cryptographic protocols

مقدمه

امنیت ارتباطات دیجیتال به جنبه‌هایی وابسته است که در آنها سازوکارهای رمزنگاشتی نقش به طور فزاینده مهمی را ایفا می‌کنند. زمانی که چنین سازوکارهایی مورد استفاده قرار گیرند، برخی از نگرانی‌های امنیتی مانند قدرت الگوریتم رمزنگاشتی‌شده، دقت و صحت اجرا، عملیات صحیح و استفاده از سامانه‌های رمزنگاشتی‌شده و امنیت پروتکل‌های رمزنگاشتی ایجاد شده وجود دارند.

پیش از این استانداردهایی درمورد مشخصات الگوریتم‌های رمزگذاری شده و برای اجرا و آزمون افزاره‌ها و پیمانه‌های رمزنگاشتی شده ایجاد شده‌اند. اگرچه هیچ استاندارد یا فرآیندی که به صورت کلی پذیرفته شده باشد برای ارزیابی مشخصات پروتکل‌های مورد استفاده در چنین ارتباطی وجود ندارد. هدف از این استاندارد ملی برقراری ابزارهایی برای تصدیق مشخصات پروتکل رمزنگاشتی شده برای ارائه سطوح تعریف شده‌ای از اطمینان پیرامون امنیت مشخصات پروتکل‌های رمزگذاری شده است.

فناوری اطلاعات- فنون امنیتی- تصدیق پروتکل‌های رمزنگاشتی

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد ملی برقراری مبنایی فنی برای اثبات امنیتی مشخصات پروتکل‌های رمزنگاشتی می‌باشد. این استاندارد ملی معیارهای ارزشیابی طراحی را برای این پروتکل‌ها و همچنین روش‌هایی که باید در فرآیند تصدیق چنین پروتکل‌هایی به‌کار گرفته شود را مشخص می‌کند. این استاندارد ملی همچنین تعاریفی را نیز درمورد سطوح تضمین مختلف سازگار با مؤلفه‌های تضمین ارزشیابی در ISO/IEC 15408 ارائه می‌دهد.

۲ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به‌کار می‌رود.

۱-۲

تعداد نشان‌وندها

تعداد نشانوندها[1]

۲-۲

پروتکل رمزنگاشتی

پروتکلی که عملکردی مرتبط با امنیت را با استفاده از رمزنگاشتی اجرا می‌کند

۳-۲

روش‌های رسمی

فنونی مبتنی بر مفاهیم ریاضی که به خوبی تثبیت شده جهت طرح ریزی ، محاسبه و تخمین که در مشخصات، طراحی، تحلیل، ساختار و تضمین سامانه‌های نرم افزاری و سخت افزاری به‌کار می‌رود.

۴-۲

شرح رسمی

شرحی که نحو و معانی آنها بر مبنای مفاهیم ریاضی به خوبی تثبیت شده، تعریف شده‌اند.

۵-۲

زبان رسمی

زبانی برای طرح ریزی، محاسبه و تخمین مورد استفاده در مشخصات، طراحی، تحلیل، ساختار و تضمین سامانه‌های نرم افزاری و سخت افزاری که نحو و معانی آنها بر مبنای مفاهیم ریاضی به خوبی تثبیت شده تعریف شده‌اند.

1- Arguments

۶-۲

مدل مخالف

شرح قدرت‌های مخالفان که می‌توانند در جهت شکست پروتکل تلاش کنند

یادآوری - این مدل شامل محدودیت‌ها در منابع در دسترس، توانایی مخالفان و غیره می‌شود.

۷-۲

ویژگی امنیتی

ویژگی به طور رسمی‌یا غیر رسمی‌تعریف شده که در آن یک پروتکل رمزنگاشتی جهت تضمین مواردی مانند رازداری، اعتبار یا گمنامی‌طراحی شده است

۸-۲

گواه خود ارزیابی

گواهی که توسعه دهنده از آن جهت بررسی اینکه آیا یک پروتکل مشخص ویژگی‌های امنیتی اختصاص داده شده به آن را برآورده می‌کند و یا خیر، استفاده می‌کند

یادآوری- این مشخصات شامل پروتکل رمزنگاری، مدل خصمانه و خروجی (رونوشت) تصدیق رسمی می‌باشد.

۹-۲

مدل پروتکل

مشخصات یک پروتکل و رفتار آن با توجه به یک مدل مخالف است.

۱۰-۲

مشخصات پروتکل

تمام شرح‌های رسمی و غیر رسمی‌یک پروتکل مشخص شده است.

یادآوری- این شامل تمام فرآیندهای استفاده شده توسط هر یک از مشترکان پروتکل، تمام ارتباطات بین آنها و ترتیب آنها می‌شود.

۱۱-۲

رازداری

ویژگی امنیتی برای یک پروتکل رمزنگاشتی به نحوی که یک پیام یا داده نباید توسط نهادهای غیرمجاز فهمیده شود.

۱۲-۲

تابعی با تعداد نشان وند های نا محدود[1]

ویژگی یک عملکرد که تعداد نشان‌وندهای آن متغیر است.

۳ نمادها و نشان گذاری

در جهت اهداف این استاندارد، نمادها و نشان گذاری زیر به‌کاربرده می‌شود.

$\emptyset$	ویژگی امنیتی یک مدل پروتکل
A,B	نام‌های نقش
m	پیام
r	واژه تصادفی
k	کلید
c	مجرای ارتباط
enc	عمل رمزنگاشتی کردن
dec	عمل کشف رمز
$<..,...>$	عامل جفت سازی
$Send$	فرآیند ارسال
$Receive$	فرآیند دریافت

۴ کلیات

تصدیق یک پروتکل رمزنگاشتی شامل بررسی محصولات زیر است:

الف) مشخصه پروتکل رمزنگاشتی؛

ب) مشخصه مدل مخالف؛

پ) مشخصه اهداف و ویژگی‌های امنیتی؛

ت) گواه خود ارزیابی که پروتکل رمزنگاشتی در مدل مخالف آن به اهداف و ویژگی‌ها دست می‌یابد و آنها را برآورده می‌کند.

محصولات باید به روشنی پارامترها یا مشخصات مرتبط برای تصدیق را بیان کنند. مثال‌ها در این زمینه شامل محدوده (مرز) مورد استفاده در تصدیق محدود است که در بند ۷-۴-۴-۱ تعریف شده است یا مشخصات جبری عامل‌های رمزنگاشتی مورد استفاده در پروتکل که در بند ۷-۱-۲-۳ و بند ۵-۳-۴ تعریف شده‌اند.

سطوح تضمین پروتکل متفاوت برای این چهار محصول به الزامات متفاوت منجر خواهد شد. الزامات بیان شده تنها برای تصدیق طراحی است نه تصدیق اجرا.

یادآوری ۱- جهت تصدیق اجرا، الزامات تضمین افزوده باید تامین و برآورده شود.

---

1 -Variadic

این استاندارد ملی با صراحت، روش‌ها یا ابزارهای اثباتی که باید مورد استفاده قرار گیرند را مشخص نکرده است، اما در عوض تنها مشخصات آنها را مشخص کرده است. این امر طراحان پروتکل را به استفاده از جدیدترین فناوری برای تصدیق پروتکل بر حسب پیمانه، روش‌ها و ابزارها تشویق می‌کند.

ابزارهای تصدیق باید شرایط زیر را برآورده کنند.

الف- ابزارهای تصدیق درست هستند.

طراح پروتکل یا احتمالا یک شخص ثالث مستقل باید گواهی برای صحت ابزار تصدیق مورد استفاده ارائه دهد. این گواه، برای مثال، می‌تواند بر حسب یک گواه کاغذ و قلم درمورد درستی حساب [1] مورد استفاده، یا در برخی موارد برحسب بازبینی کد جهت بررسی اینکه ابزار به درستی حساب را اجرا کرده است، باشد.

یادآوری ۲- این گام کوچک اما نه بی اهمیت است، در عین حال اگر گواه‌هایی که با ماشین بررسی شده‌اند جهت فراهم آوردن اطمینان بیشتر نسبت به گواه‌های دستی باشند، ضروری است. به صورت نظری، این امر می‌تواند یکبار و برای همیشه برای یک ابزار تصدیق صورت گیرد، اگرچه در عمل، ابزارها طی زمان استنتاج می‌شوند.

ب- نتایج ابزارهای تصدیق به روشی مستند می‌شوند که قابل تکرار باشند.

طراح پروتکل باید مستند سازی مناسب را شامل تمام ورودی‌های مورد نیاز برای ابزار جهت ساخت یک گواه (در مورد رویه‌های تصمیم گیری) یا تعیین قابلیت اثبات ارائه دهد.

پ- ابزارهای تصدیق برای ارزیابی و استفاده خارجی در دسترس هستند.

طراح پروتکل باید تمام ابزارهای ضروری جهت بررسی مستقل گواه‌ها را نشان دهد.

یادآوری ۳- حداقل به صورت تئوری، تصدیق پروتکل می‌تواند به وسیله گواه‌های دستی با استفاده از کاغذ و قلم انجام شود. اگرچه، میزان قابل توجه تعیین شده جزئیات که نوعا در تصدیق پروتکل امنیتی وجود دارد، به ویژه برای سطوح تضمین پروتکل سطح بالا، اطمینان در نتایج با استفاده از ابزارهای مکانیزه شده مانند علامت گذارهای [2] مدل و اثبات کننده‌های نظریه به صورت قابل توجهی افزایش می‌یابد. از این رو، گواه‌ها تنها با استفاده از کاغذ و قلم با سطح تضمین پایین تری (یعنی PAL2) نسبت به گواه مکانیزه شده در این استاندارد ملی تلقی می‌شود.

۵ مشخص کردن پروتکل‌های رمزنگاشتی

۵-۱ اهداف

هدف از این قسمت ارائه رهنمودها و حداقل الزامات در مشخص کردن پروتکل‌های رمزنگاشتی است.

۵-۲ سطوح انتزاعی [3]

پروتکل‌ها می‌توانند در چندین سطح انتزاعی، هریک از سطوح مطابق با یک مدل محاسبه، مشخص شوند. در مجردترین سطح(خلاصه انتزاعی)، پیام‌ها اصطلاحاتی هستند که از نشانه‌ها ساخته می‌شوند و مهاجم نیز به عنوان یک فرآیند رسمی‌طرح ریزی می‌شود. این انتزاعی سطح نمادین نامیده خواهد شد. در چنین مدلی، منابع (منابع زمان و مکان هردو) درنظر گرفته نمی‌شوند.

1- calculus
2- checkers
3- abstraction

هر مدل دیگری می‌تواند به عنوان پالایش مدل نمادین تعریف شود. برای مثال می‌توان نشانه‌های مورد استفاده در مدل نمادین را به عنوان عملکردها برروی رشته‌های بیتی که می‌تواند در چندجمله‌ای زمان محاسبه شود، تفسیر کرد.

از این رو، هر پروتکل رمزنگاشتی در یک مشخصه نمادین و یک تفسیر در یک دامنه معین (برای مثال، رشته‌های بیتی یا داده دارای ساختار یا حتی قالب‌های وابسته به ماده) از تمام نشانه‌ها، همراه با فرضیات درمورد تفسیر آنها مرکب است. چنین فرضیه‌ای می‌تواند برخی مطابقت‌ها را میان ویژگی‌ها در سطوح انتزاعی گوناگون تضمین کند.

یادآوری- در این استاندارد ملی تنها مشخصه نمادین پروتکل‌های امنیتی مدنظر قرار داده شده است.

اسناد بیشتری برای مشخصه دیگر سطوح انتزاعی (سطح پایین تر) مورد نیاز است. نوعا، تعریف چگونگی مشخص کردن دامنه تفسیر و چگونگی اجرای تضمین‌های امنیتی در تمام سطوح انتزاعی ضروری خواهد بود.

۵-۳ مشخصه پروتکل‌های امنیتی

۵-۳-۱کلیات

همانطور که شرح داده شده، یک مشخصه نمادین اولین قسمت ضروری در مقابل مشخصه کامل یک پروتکل است. در فهرست زیر حداقل قسمت‌های الزامی‌در یک مشخصه پروتکل نمادین بیان شده است.

۵-۳-۲ پیام‌های نمادین

قسمت اول شامل مشخص کردن پیام‌های امکان پذیر (معتبر) است.

در این بند، توابع اولیه رمزنگاشتی مورد استفاده در این پروتکل باید به صورت فهرست بیان شود. از آنجایی که بحث پیرامون یک مشخصه نمادین است، این قسمت متشکل از ارائه‌های زیر است.

۱- مجموعه‌ای از نشانه‌های عملکرد $\mathcal{F}$

هر نشانه عملکرد یا دارای یک **تعداد نشان‌وندهای** ثابت است، که باید تعیین شود، یا تابعی با تعداد نشان‌وندهای نامحدود است (که در این مورد نیز باید تعیین شود).

۲- مجموعه‌ای از *نشانه‌های نام* $\mathcal{N}$ که می‌تواند به چندین دسته نحوی گوناگون تقسیم شود که باید تعیین شوند.

۳- مجموعه از *نشانه‌های متغیر* $\mathcal{X}$

۴- تعریف رسمی قواعد معتبر که امکان ساخت پیام‌ها با استفاده از نشانه‌های عملکرد را ایجاد می‌کند. یک فهرست (غیر جامع) از روش‌های امکان پذیر جهت تعیین اینکه چنین زبانی به صورت موارد زیر است:

- هیچ[1]: تمام اصطلاحاتی که با نشانه‌های عملکرد ساخته می‌شوند و محدودیت‌های تعداد نشان‌وندهای را دنبال می‌کنند، پیام‌های معتبر هستند
- برخی از متغیرها به نام‌ها محدود می‌شوند: برخی از متغیرهای نشانه‌های عملکرد محدود به وابسته بودن به برخی از دسته‌های نام است

1- nothing

- دسته‌ها: یک نظم طبقه تعریف می‌شود و تنها اصطلاحات به خوبی طبقه بندی شده به پیام‌ها مرتبط هستند.

مجموعه اصطلاحات (یا پیام‌ها) معتبر ($\mathcal{F}, \mathcal{N}$) یا ($\mathcal{F}, \mathcal{N}, \mathcal{X}$) زمانی که متغیرها مورد بحث هستند)

مثال- نمونه مثال رمزنگاشتی است، که می‌تواند به وسیله نشانه enc که تعداد نشان‌وندهای آن ۲ یا ۳ (یا ۴) است بسته به اینکه آیا رده بندی تصادفی روشن است یا خیر (و اینکه آیا الگوریتم رمزنگاشتی روشن است و یا خیر) شکل می‌گیرد. یک مشخصه باید معین کند که تعداد نشان‌وندهای، enc چیست و انواع فرضی متغیرهای آن کدام‌ها هستند. نوعا enc دارای تعداد نشان‌وندهای ۳ است. به عنوان طبقه‌های نام احتمالی رده بندی‌های تصادفی وجود دارند که نشانه‌های آن با r آغاز می‌شود، کلیدهایی که نشانه‌های با k آغاز می‌شود، الگوریتم‌هایی که نشانه‌های آن با α آغاز می‌شود و غیره. درصورتی که enc به صورتی معین شود که نشانه تعداد نشان‌وندهای ۳ باشد، می‌توان به صورت افزوده برای مثال با مشخص کردن اینکه اولین متغیر باید یک کلید و آخرین آن باید تصادفی باشد، متغیرهای آن را محدود کرد. در این مورد enc (k,k,r)، enc (k,enc(k, r_1, r_2), r_1)، اصطلاحات معتبر هستند درحالی که enc (enc (k, k',r), k'',r') و enc (r,k,r') اصطلاحات معتبر نیستند. مثال‌هایی از نشانه‌ها می‌توانند به صورت تابعی با تعداد نشان‌وندهای نامحدود شامل تابع انحصاری یا $\oplus$ ، ضرب حسابی × یا الحاق || مدنظر قرار می‌گیرند.

۵-۳-۳ پیام‌های مشاهده شده

در این قسمت گزاره‌های مقایسه‌ای میان پیام‌ها مشخص می‌شوند.

تنها گزاره تساوی الزامی‌است، چرا که دیگر گزاره‌ها می‌توانند به عنوان توابع بولی درک و در تعریف تساوی مشخص شوند. اگرچه ممکن است این امر جهت تشخیص پس از آن میان توانایی‌های رایانشی و مشاهداتی مفید باشد. به علاوه، در بسیاری از زبان‌های مشخصه حال حاضر، ویژگی‌های نشانه‌های تابع به صورت معادلاتی (به بند ۵,۳,۴ مراجعه شود) مشخص می‌شوند، درحالی که مشخص کردن معادله‌ای توانایی‌های مشاهده‌ای می‌تواند غیر ممکن باشد.

این قسمت متشکل از فهرستی از نشانه‌های گزاره، همراه با تعداد نشان‌وندهای آنها است. نمونه مثال‌ها شامل گزاره‌های طبقه بندب، تساوی و same_length (که داشتن طول یکسان دو متغیر آن را بررسی می‌کند)، same_key (که رمزنگاشتی شدن دو خروجی داده یک رمز را با کلید یکسان بررسی می‌کند).

۵-۳-۴ ویژگی‌های جبری

این قسمت مشخص می‌کند چه زمانی دو اصطلاح معتبر پیام یکسانی را نمایش می‌دهد و به صورت کلی تر، تفسیرهای نشانه‌های گزاره بیان شده در بند پیش کدام‌ها هستند.

برای مثال، زمانی که نشانه‌های تابع شامل هر دو مورد رمزنگاشتی و رمزگشایی (متقارن) هستند، ممکن است تعیین $\mathrm{dec}(k,\mathrm{enc}(k,x,r))=x$ درنظر گرفته شود که در آن r نمادین برای یک رده بندی تصادفی جهت بیان رمزنگاشتی احتمالی است: این موارد نمایش‌های دو جمله‌ای یک پیام است. همچنین ممکن است تعیین اینکه $x \oplus x=0$ درنظر گرفته شود اگر استفاده از نشانه $\oplus$ برای نمایش تابع یای مانع جمع[1] درنظر گرفته شده باشد.

1- exclusive

به طور معمول، فرض براین است که هر دو جمله که به عنوان مساوی مشخص نشده‌اند متفاوت هستند. نقش مشابهی نیز برای گزاره‌ها به‌کار برده می‌شود: هرچیزی که به عنوان صحیح مشخص نشده باشد، به صورت پیش فرض غلط است.

۵-۳-۵ نقش‌های پروتکل

یک نقش برنامه‌ای تعاملی است که برخی ورودی‌ها را از محیط دریافت می‌کند و پیام‌هایی را به محیط ارسال می‌کند. این مؤلفه برنامه هسته‌ای یک پروتکل است که : هیچ ارتباطی درون یک نقش رخ نمی‌دهد.

مشخص کردن یک نقش مستلزم ارائه موارد زیر است:

۱- یک نام نقش؛

۲- فهرستی محدود از پارامترهای رسمی: این پارامترها داده‌هایی هستند که می‌توانند بدون تولید شدن یا دریافت شدن از محیط به وسیله برنامه مورد استفاده قرار گیرد؛

۳- مجموعه‌ای (معمولا محدود، اما الزامی‌برای محدودیت وجود ندارد) از کنترل حالت‌ها؛

۴- مجموعه‌ای از متغیرهای محلی و نام‌های محلی؛

۵- مشخصه‌ای از توانایی‌های ارسال و دریافت و همچنین تراکنش‌های حالت؛

۶- به صورت رسمی‌این مقادیر جهت مشخص کردن روابط $q, v \xrightarrow{send\,(c,m)} q', v'$ ، و $q, v \xrightarrow{receive\,(c,m)} q', v'$ یک مجرای ارتباطاتی c و یک پیام m ایجاد می‌شوند.

چنین مشخصه‌ای برای هیچ زبان برنامه نویسی خاص یا هیچ روش خاص جهت اجرای آزمون‌ها یا حرکات به‌کار برده نمی‌شود. این امر تنها مستلزم مشخصه داده واردکردن/خارج کردن و ارتباطات با محیط است.

مثال- این یک مشخصه احتمالی نقش پاسخگو در پروتکل Needham-Schroeder است. یک مجرای ارتباطی منفرد، که در زیر حذف شده است فرض می‌شود.

۱- نام نقش : B؛

۲- پارامترها: شناسه b عامل اجرا کننده نمونه‌این نقش، شناسه a، کلید خصوصی b، کلید عمومیa؛

۳- حالت‌های محلی: تنها ۳ حالت محلی وجود دارد: q_0, q_1, q_f؛

۴- متغیرها و نام‌های محلی: n_B, r نام‌های محلی و x, y متغیرهای محلی هستند

یک مشخصه تراکنش‌ها. هر زبان به صورت رسمی‌تعریف شده دیگر می‌تواند در اینجا جانشین شود:

$$q_0, n_B, r, x = 0, y = 0 \xrightarrow{\text{Receive}(m)} q_1, n_B, r, x = m, y = 0$$

$$q_1, n_B, r, x = m, y = 0 \xrightarrow{\text{Send}\left(\text{enc}(\text{pub}(a),\langle m', n\rangle, r)\right)} q_f, n_B, x = m, y = m'$$

$$\text{if } a = \pi_1\left(\text{dec}(\text{priv}(b), x)\right), m' = \pi_2(\text{dec}(\text{priv}(b), x))$$

در اینجا از یک نشانه رمزنگاشتی در مبنای سه enc، یک نشانه رمزگشایی dec، یک نشانه جفت سازی $< -, - >$ و نشانه‌های طرح ریزی π_1, π_2 استفاده می‌شود.

یادآوری- درچنین مثالی، زمانی که آزمون با شکست مواجه می‌شود تراکنش مشخص نمی‌شودف به این معنا که هیچ تراکنشی در این مورد وجود ندارد: برنامه در حالت q_1 انباشته شده است. مطمئنا طراحی‌های ممکن دیگری نیز وجود دارد.

دوره‌ها یک نمونه نقش کپی خاص از یک نقش، همراه با پارامترهای اصلی آن است. این نمونه در برخی موارد دوره نامیده می‌شود. از آنجایی که شناسه یکسان می‌تواند به صورت همزمان چندین کپی از نقش یکسان را اجرا کند، ممکن است قرار دادن یک شناساگر که برخی مواقع شماره دوره نیز نامیده می‌شود در پارامترها مناسب خواهد بود، که شناسایی شدن نمونه‌های نقش مختلف را امکان پذیر خواهد کرد.

۵-۴ مشخصه مدل مخالف

۵-۴-۱ مشخصه شبکه

در این قسمت افزاره‌های ارتباطاتی (نشانه ای) و قابلیت اطمینان آنها مشخص می‌شود.

نوعا، فهرستی از مجراها (اصطلاحات یا نشانه‌ها) تعیین می‌شوند، هریک از آنها دارای ویژگی‌های خود است. برای مثال، یکی از این موارد می‌تواند یک مجرای ارتباطی عمومی‌منفرد c را که تحت کنترل کامل مهاجم (که می‌تواند پیام‌ها را قطع و پیام‌های جعلی را ارسال کند) مشخص کند. اما با تشخیص یک مجرای ارتباطی پروکسی ایمن تر (یا با ایمنی کمتر!) یا یک مجرای بی سیم که تنها می‌تواند مورد استراق سمع قرار گیرد یا حتی یک مجرای خصوصی که کاملا خارج از کنترل یک مهاجم است، بیشتر تصفیه[1] شود.

۵-۴-۲ مهاجم

این قسمت توانایی‌های رایانشی مهاجم نشانه‌ای را مشخص می‌کند. به بیان دیگر، پیام‌های m را که می‌توانند از یک مجموعه از پیام‌های S رایانش شوند، مشخص می‌کند.

مشخصات نوعی از سامانه‌های استنتاج مانند «سامانه استنتاج Dolev-Yao» استفاده می‌کنند. این قواعد ممکن است برای مثال به اینکه آیا یک نشانه رمزگشایی آشکار وجود دارد و یا خیر بستگی داشته باشد. ساده ترین مشخصه عبارت است از داشتن تمام نشانه‌های عملکرد آشکار و عمومی. سپس مهاجم، هنگام تعیین یک مجموعه از نام‌های $\mathcal{N}$ ، قادر است هر اصطلاح ساخته شده بر اساس $\mathcal{F}$ و $\mathcal{N}$ رایانش کند.

به علاوه، مهاجم می‌تواند از نشانه‌های گزاره‌ای بند ۵-۳-۳ با اینکه چنین گزاره‌هایی در تعریف نقش‌ها مورد استفاده قرار نمی‌گیرند، استفاده کند. قابلیت‌های دیگر مهاجم در بند ۵-۴-۱ مشخص شده‌اند و به قابلیت اطمینان مجراهای مختلف بستگی دارند.

از این بند و بند قبل، باید تعریف رسمی‌اینکه ردیابی‌هایی اجرایی امکان پذیر کدام‌ها هستند، میسر باشد.

یادآوری ۱- نمونه حمله‌ها می‌توانند به طور رسمی‌به صورت زیر شرح داده شوند.

حمله استراق سمع یک نمونه از خطر امنیتی است که شبکه‌ها در معرض آن قرار دارند. در قسمتی از محیط شبکه، پیام‌ها برای همه منتشر می‌شوند. این امر اغلب می‌تواند موجب ایجاد مشکلی شود که پیام‌های مهم مانند رمزهای عبور و شماره‌های کارت اعتباری ممکن است به شخص پیش بینی نشده تحویل شود. این حمله می‌تواند به صورت رسمی‌به عنوان زیرمجموعه مدل بند ۵-۴-۱ شرح داده شود. یعنی، با تعیین فهرستی از مجراهای $\{c\}$ یک مهاجم هیچ کنترلی بر مجراهای $\{c\}$ ندارد اما می‌تواند به تمام پیام‌های S تبادل شده میان مجراها گوش دهد. سپس، تمام آگاهی مهاجم، هر اصطلاحی است که می‌تواند از یک مجموعه از پیام‌های S رایانش شود.

---

1 -refined

حمله پاسخ نوع دیگر خطر است. در شبکه‌های باز مانند اینترنت، پیام‌ها می‌توانند از طریق مسیریاب‌هایی که تحت کنترل فرد دارای سوء نیت است مبادله شوند. در چنین محیطی، پیام‌ها مانند رمزهای عبور یا شماره‌های کارت اعتباری که در یک شبکه تبادل می‌شوند می‌توانند از طریق آنها با سوءنیت تکرار شود و یا تاخیر داشته باشد. این امر اغلب موجب ایجاد این مشکل می‌شود که فرد پیش بینی نشده‌ای با تکرار رمزعبور ذخیره شده به عنوان گواه شناسه هویت فرد قانونی را جعل کند. این حمله می‌تواند به صورت رسمی‌به عنوان مدل بند ۵-۴-۱ و زیرمجموعه مدل در بند ۵-۴-۱ شرح داده شود. یعنی فهرستی از مجراهای $\{c\}$ و یک مجموعه از پیام‌های S در مجراهای $\{c\}$ تبادل می‌شود، یک مهاجم دارای کنترل کامل بر مجراهای $\{c\}$ است و به تمام پیام‌های S گوش می‌دهد. از این رو، آگاهی کامل از مهاجم هر اصطلاحی است که می‌تواند از یک مجموعه از پیام‌های S رایانش شود. اما، در حمله پاسخ، مهاجم تنها از عناصر S استفاده و سعی می‌کند قسمتی از نقش را تقلید کند.

یادآوری ۲- توسعه مدل مستلزم شرح دادن سلسله حملات مانند حمله رد سرویس و حمله اعتماد است. از آنجایی که این حملات به ویژگی‌های فیزیکی یک سامانه واقعی مانند زمان پردازش عملیات‌ها و سرعت ارتباط از طریق رسانه فیزیکی، به منظور شرح چنین حملاتی مرتبط است، چنین ویژگی‌های فیزیکی باید به نوعی در مدل توسعه یافته وجود داشته باشد.

۵-۴-۳ سناریو

آخرین قسمت در مشخصه پروتکل عبارت است از شرح محیط‌های اجرا که مدنظر قرار می‌گیرند.

به صورت کلی این قسمت شامل ویژگی‌های مهم زیر می‌شود:

- دانش اولیه مهاجم: یک مجموعه از پیام‌ها.
- چگونه نقش‌ها (و به صورت کلی تر فرآیندهای مرکب) ساخته شده‌اند.

در مثال‌های نوعی، نقش‌ها می‌توانند به صورت همزمان اجرا شوند. از این رو یک عامل ترکیب موازی مورد استفاده قرار می‌گیرد. اما دیگر موقعیت‌ها می‌توانند وابسته باشند: برخی مراحل/شیوه‌ها مانند پروتکل رأی گیری الکترونیکی یا امضای قرارداد می‌تواند وجود داشته باشد که در هر مورد ترکیب‌های متوالی یا حتی ترکیب مشروط ممکن است مورد نیاز باشد.

- چگونه نقش‌ها (و به صورت کلی تر فرآیندهای مرکب) می‌توانند تکرار یا به صورت پویا ایجاد شوند.

منظور از«تکرارشدن P» این است که تعداد نامحدودی از کپی‌های P می‌توانند به صورت همزمان اجرا شوند. این امر می‌تواند در سناریو مورد توجه امکان پذیر باشد و یا نباشد و باید دقیق باشد. قیدهای مشابهی باید برای تعداد شناسه‌های مجزا مشخص شود.

- پنهان کردن یا به اشتراک گذاری نام‌ها.

این قسمت مشخص می‌کند که کجا داده تولید شده و چگونه موروثی شده است. برای مثال فرض براین است که نقش P به یک پارامتر k (یک کلید) وابسته است. تفاوت زیادی میان تولید k[1] (تکرار) $(P(k)$[2] و (تکرار) P (k)

1- generate k

2- replicate

وتولید k P(k) وجود دارد. در مورد قبلی، هر کپی تکرار شده P کلید یکسان k را در اختیار دارد. در مورد بعدی، هر کپی از P کلید k خود را تولید می‌کند. ساختار تولید نام نه تنها با تعیین دامنه نام فراهم می‌شود، بلکه به عنوان یک متصل کننده عمل می‌کند: در آن محدوده، نام می‌تواند با یک مورد جدید جایگزین شود. این امر در تشخیص نمونه‌هایی که به صورت محلی نام‌ها را تولید می‌کنند ضروری است.

سپس برای مشخصه ویژگی‌های امنیتی، نیاز به تمایز میان عوامل صادق، عوامل متقلب، عامل‌هایی که می‌توانند معیوب شوند و غیره نیاز خواهد بود. توانایی تخریب نیز ممکن است در این سناریو مشخص شوند، اما به‌طور دقیق از ابتدای رده نام‌ها و اجراهای نقش مختلف، به اینکه آیا از سوی عامل معیوب اجرا شود و یا خیر بستگی دارد.

۵-۵- مشخصه ویژگی‌های امنیتی

۵-۵-۱ کلیات

نظر به تنوع بسیار زیاد ویژگی‌های امنیتی (در تمام سطوح انتزاعی)، به نظر نمی‌رسد درحال حاضر تعیین یک روش کلی برای شرح ویژگی‌های امنیتی امکان پذیر باشد. به علاوه، درحال حاضر هیچ روشی برای مشخص کردن ویژگی‌های امنیتی (حتی موارد ساده)، مستقل از زبان مشخصه پروتکل وجود ندارد.

دو بند ویژگی‌ها به اندازه کافی برای مشخصه رسمی‌کامل به نظر می‌رسد:

- ویژگی‌های ردیابی: این ویژگی‌ها به طور اساسی بیان می‌کند که در هر اجرای احتمالی، هیچ رویداد بدی رخ نمی‌دهد. این ویژگی‌ها مورد رده‌ای مدل بررسی ویژگی‌های زمان خطی است.
- ویژگی‌های هم ارزی: این ویژگی‌ها نشان می‌دهند که مهاجم نمی‌تواند هر اطلاعات مرتبطی را در مورد یک داده معین بدست آورد. چنین ویژگی‌هایی با استفاده از دو آزمایش، که هر یک از آنها با نقش‌های یکسان برابر است، اما با یک سناریو متفاوت، رسمی می‌شوند[1]. مهاجم نباید بتواند دو آزمایش را از یکدیگر تشخیص دهد. چنین ویژگی غیرقابل تشخیصی با مفهوم رده‌ای (کلاسیک) هم ارزی مبنی بر مشاهده در نظریه همزمانی مطابق است.

ما به طور مختصر برای ویژگی‌های ردیابی برخی از خصیصه‌های مهم و اطلاعات مرتبط برای مشخصه را مورد تحقیق قرار می‌دهیم.

۵-۵-۲ ویژگی‌های ردیابی

در هر زمان، وضعیت کلی شبکه می‌تواند با استفاده از جمع آوری پیکربندی‌های هر نمونه نقش، سناریو جاری و دنبال S تمام پیام‌هایی که تا کنون در مجراها ارسال شده‌اند که می‌توانند مورد استراق سمع قرار گیرند شرح داده شوند.

ویژگی لحظه‌ای در چنین حالت کلی یک گزاره است. برای مثال، $P(s)$: « یک پیام مشخص از S به وسیله مهاجم قابل رایانش است». چنین ویژگی‌هایی می‌تواند به رویدادها اشاره داشته باشد.

1- formalized

ویژگی موقتی ترکیبی از ویژگی‌های لحظه‌ای، با استفاده از کیفیت‌های موقتی است. برای مثال $\Phi(s)$: « $P(s)$ هرگز رخ نمی‌دهد»، یا «هر زمان $P(s)$ رخ می‌دهد، پیش از رخ داد $Q(t)$ است».

ویژگی ردیابی با یک ویژگی موقتی تعیین کیفیت شده تعریف می‌شود: «برای هر نام $\Phi(s)$ n,...,». پیچیده ترین تعیین کیفیت‌ها ممکن است مورد نیاز باشد.

۱- مشخص کردن ویژگی‌های ردیابی مستلزم موارد زیر است

۲- مشخص کردن یک یا چند رویداد (پارامتری شده)؛

۳- مشخص کردن مجموعه‌ای از برنامه‌های زمانبندی چنین رویدادهایی؛

۴- مشخص کردن اینکه برای کدام مقادیر پارامترها ویژگی موقتی باید نگه داشته شود.

مثال- ابتدا به صورت غیررسمیو سپس به صورت رسمییک ویژگی توافق مشخص می‌شود. در هر نمونه از نقش پاسخ دهنده در پروتکل Needham-Shroeder، درصورتی که متغیر y آن نمونه برای 'm در برخی نقاط صدق می‌کند، و در صورتی که هر دو شناسه که پارامترهای آن نقش هستند صادق باشند، پیش از آن رویداد، a باید 'm را برای b تولید کند.

به طور رسمی، دو رویداد مورد استفاده قرار می‌گیرد: $P(b,a,m)$ و $Q(a,b,m)$. اولین رویداد زمانی صدق می‌کند که یک نمونه نقش موجود باشد که نام آن B است و پارامترها شامل دو شناسه b و a می‌شوند و به طوری که متغیر محلی y، m اختصاص داده شده است. رویداد دوم زمانی صادق است که یک نمونه نقش موجود باشد که نام آن A و پارامترهای شامل دو شناسه a و b می‌شوند و به طوری که متغیر محلی x، m اختصاص داده شده است.

ویژگی موقتی سپس بیان می‌کند که $\neg P(b,a,m)\ U\ Q(a,b,m)$: هیچ رویداد $P(b,a,m)$ وجود ندارد تا زمانی که یک رویداد $Q(a,b,m)$ رخ دهد. در نهایت، ویژگی تصدیق (توافق) نشان می‌دهد که برای هر پیام m و هر شناسه صادق a و b صدق می‌کند. شناسه‌های صادق (.resp غیرصادق) اینجا، رده‌های نام متمایز فرض می‌شوند. ویژگی‌های توافقی پیچیده تر ممکن است مستلزم رجوع به شماره‌های دوره باشند و در اینجا گزارش نشده‌اند.

۶ سطوح تضمین پروتکل رمزگذار

۶-۱ کلیات

هدف از این استاندارد ملی ارزیابی امنیت پروتکل‌های رمزنگاشتی در یک سطح مشخصه است. این امر به آماده سازی محیطی منجر می‌شود که پروتکل‌های رمزنگاشتی می‌توانند به عنوان قسمتی از یک سامانه کلی مورد استفاده قرار گیرند، درحالی که این قسمت می‌تواند به عنوان یک جعبه سیاه مجاز امنیتی مورد توجه قرار گیرد. در [13,14,15] ISO/IEC 15408، هنگام ارزیابی محصولات فناوری اطلاعات عمومی، اثبات امنیت یک پروتکل رمزنگاشتی استاندارد مورد استفاده در محصولات الزامی‌نیست، درحالی که یک پروتکل رمزنگاشتی اختصاصی مورد استفاده در محصولات جهت نشان دادن در چهارچوب ISO/IEC 15408 مورد نیاز است که می‌توانند ویژگی‌های امنیتی شرح داده شده در هدف امنیتی را برآورده کند. درحالی که چهارچوب ISO/IEC 15408 نه تنها برای طراح جهت نشان دادن ویژگی امنیتی مشخصه مورد نیاز است، بلکه مستلزم تصحیح اجرا است، که اغلب وظایف گوناگونی را اتخاذ می‌کند. بنابراین، این استاندارد ملی مبنای متداولی را برای تصدیق ویژگی امنیتی مشخصه ارائه می‌دهد. این استاندارد ملی تضمین سطح بالایی را در مورد مشخصه یک پروتکل اختصاصی مبتنی

بر روش‌های سخت تصدیق ارائه می‌دهد، از این رو استفاده از یک پروتکل رمزنگاشتی اختصاصی را در یک سامانه به عنوان یک جعبه سیاه مجاز امنیتی امکان پذیر می‌کند که به اندازه پروتکل‌های رمزنگاشتی استانداردی که به طور متداول مورد استفاده قرار می‌گیرند مطمئن است.

یادآوری- هریک از چهار محصول در این استاندارد ملی با ISO/IEC 15408 و ISO/IEC 18045 به صورت پیش رو مطابقت دارند: (۱) مشخصه پروتکل رمزنگاشتی می‌تواند به عنوان قسمتی از عاملیت امنیتی TOE (TSF)[1] شناسایی شود. (۲) مدل مخالف می‌تواند به عنوان قسمتی از محیط عملیاتی که در آن پروتکل با تعامل احتمالی با یک مهاجم که توانایی آن در مدل مشخص شده است اجرا می‌شود. (۳) ویژگی امنیتی می‌تواند به عنوان قسمتی از مدل خط مشی امنیتی (SPM)[2] رسمی‌و غیر رسمی‌مبتنی بر الزامات عملیاتی امنیتی (SFR)[3] که پروتکل باید آن را برآورده کند، مانند محرمانه بودن کلید تبادل شده و اعتبار قسمت ارتباطی و غیره شناسایی شود. (۴) گواه خود ارزیابی می‌تواند به عنوان قسمتی از گواه شناسایی شود، یعنی آنچه طراح پروتکل در مشخصه پروتکل به عنوان قسمتی از TSF شرح داده است ویژگی امنیتی مشخص شده به عنوان قسمتی از SPM را در مدل مخالف مشخص شده به عنوان قسمتی از محیط عملیاتی برآورده می‌کند.

در قسمت زیر ۳ سطح از الزامات تضمین در محصولات طراحی بیان می‌شود که ضمانت‌های به صورت فزاینده قدرتمندی را در مورد امنیت پروتکل‌های رمزنگاشتی ارائه می‌دهد. این سطوح دارای الزامات وابسته هستند.

1- TOE Security Functionality

2- Security Policy Model

3- Security Functional Requirement

جدول ۱- سطوح تضمین پروتکل رمزنگاشتی

سطح تضمین پروتکل	PAL1	PAL2	PAL3	PAL4
مشخصه پروتکل	PPS_SEMIFORMAL شرح نیمه رسمی‌مشخصه پروتکل	PPS_FORAML شرح رسمی‌مشخصه پروتکل	PPS_MECHANIZED شرح رسمی‌مشخصه پروتکل به یک زبان مشخصه ویژه ابزار، که نحوهای آن به صورت ریاضی تعریف شده‌اند.	
مدل مخالف	PAM_INFORMAL شرح غیررسمی‌مدل مخالف	PAM_FORMAL شرح رسمی‌مدل مخالف	PAM_MECHANIZED شرح رسمی‌مدل مخالف به یک زبان مشخصه ویژه ابزار، که نحوهای آن به صورت ریاضی تعریف می‌شوند.	
ویژگی امنیتی	PSP_INFORMAL شرح غیر رسمی‌ویژگی امنیتی	PSP_FORAML شرح رسمی‌ویژگی امنیتی	PSP_MECHANIZED شرح رسمی‌ویژگی امنیتی به یک زبان مشخصه ویژه ابزار، که نحوهای آن به صورت ریاضی تعریف می‌شوند.	
گواه خود ارزیابی	PEV_ARGUMENT استدلال غیررسمی‌که مشخصه پروتکل رمزنگاشتی در مدل مخالف خود اهداف و مشخصات خود را بدست می‌آورد و برآورده می‌کند.	PEV_HANDPROVEN گواه کاغذ و قلم به صورت ریاضی رسمی‌تصدیق شده به وسیله انسان که در آن مشخصه پروتکل رمزنگاشتی در مدل مخالف آن اهداف و ویژگی‌های آن را بدست می‌آورد و برآورده می‌کند.	PEV_BOUNDED تصدیق محدود شده به کمک ابزار که مشخصه پروتکل رمزنگاشتی در مدل مخالف خود اهداف و مشخصات خود را بدست می‌آورد و برآورده می‌کند.	PEV_UNBOUNDE تصدیق غیر محدود به کمک ابزار که مشخصه پروتکل رمزنگاشتی در مدل مخالف خود اهداف و مشخصات خود را بدست می‌آورد و برآورده می‌کند.

۶-۲ سطح ۱ تضمین پروتکل

الف- قسمت‌های مربوط به امنیت پروتکل باید در یک زبان نیمه رسمی‌مشخص شود، برای مثال به عنوان دنباله‌ای از پیام‌های تبادل شده.

ب- مشخصه غیررسمی‌مدل مخالف.
پ- مشخصه غیررسمی‌ویژگی‌های امنیتی.
ت- استدلال غیررسمی‌درمورد اینکه چرا پروتکل دارای ویژگی‌های مشخص شده است.

۶-۳سطح ۲ تضمین پروتکل

الف- قسمت‌های مربوط به امنیت پروتکل باید در یک زبان رسمی‌مشخص شوند.
ب- مدل مخالف مشخص شده در یک زبان رسمی.
پ- ویژگی‌های مشخص شده در یک زبان رسمی.
ت- گواه کاغذ و قلم به صورت ریاضی رسمی‌درمورد اینکه چرا پروتکل دارای ویژگی‌های مشخص شده است.

۶-۴ سطح ۳ تضمین پروتکل

الف- قسمت‌های مرتبط با امنیت پروتکل باید در یک زبان مشخصه ویژه ابزار رسمی‌مشخص شود. مدل پروتکل ممکن است تعداد نمونه‌های نقش را به قسمتی از مقدار مشخص شده محدود شود.
ب- مدل مخالف مشخص شده در یک زبان رسمی.
پ- ویژگی‌های مشخص شده در یک زبان رسمی.
ت- گواه خود ارزیابی برای تصدیق (حل مسئله بررسی مدل) به وسیله یک ابزار بررسی مدل یا اثبات نظریه.

۶-۵ سطح ۴ تضمین پروتکل

الف- قسمت‌های مرتبط با امنیت پروتکل باید در یک زبان مشخصه ویژه ابزار رسمی‌مشخص شود. مدل پروتکل باید تعداد بسیار زیاد نامحدود نمونه‌های نقش امکان پذیر باشد
ب- مدل مخالف مشخص شده در یک زبان رسمی.
پ- ویژگی‌های مشخص شده در یک زبان رسمی.
ت- گواه خود ارزیابی برای تصدیق یا به وسیله یک ابزار بررسی مدل یا به وسیله یک ابزار اثبات نظریه. برای بررسی مدل، رویه‌هایی باید به‌کار گرفته شود که می‌تواند فضای وضعیت نامحدود را که در تصدیق نامحدود به وجود می‌آید را به‌کارگیرند.

۶-۶ تفاوت میان سطوح تضمین پروتکل

تفاوت میان PAL1 و PAL2 این است که آیا تمام جنبه‌های شرح پروتکل، مانند مشخصه، ویژگی امنیتی و مدل مخالف به صورت رسمی‌شرح داده شده‌اند و یا خیر. درصورتی که این موارد به اندازه کافی رسمی‌نباشند، تحلیل دقیق امکان پذیر نیست و طراح نمی‌تواند حملات یا گواه‌های صحت ساختار را جستجو کند. در بهترین حالت، طراحی می‌تواند ضعف نوعی را جستجو کند و با توجه به آن حملاتی که فکر طراح را به خود مشغول کرده است پروتکل را بسنجد. از این رو، PAL1 تنها کمترین ضمانت‌ها را در مورد امنیت پروتکل ارائه می‌دهد. اگرچه، PAL1 می‌تواند برای قسمتی از محیط بسته شبکه، مانند اینترانت شرکت، فاقد رقیبان متعهد کافی باشد.
در مقابل، در PAL2 و سطوح بالاتر، طراح پروتکل یک مشخصه رسمی‌را ارائه می‌دهد. این امر جستجو برای حملات را به طور دقیق یا گواه‌های صحت ساختار را امکان پذیر می‌کند.

تفاوت میان PAL2 و PAL3 این است که آیا امنیت پروتکل به صورت دستی یا با استفاده از ابزارهای مکانیکی تصدیق شده است. حداقل به صورت نظری، تصدیق پروتکل می‌تواند از طریق گواه‌های دستی، با استفاده از کاغذ و قلم صورت گیرد. اگرچه، تعیین میزان قابل توجه جزئیات که نوعا در تصدیق پروتکل رمزنگاشتی، دخیل است گواه‌های دستی می‌توانند در معرض خطا باشند و اطمینان در نتایج به صورت اساسی با استفاده از ابزارهای مکانیکی مانند بررسی کننده‌های مدل و اثبات کننده‌های نظریه افزایش می‌یابد. بنابراین، گواه‌هایی که تنها با کاغذ و قلم صورت می‌گیرند به عنوان سطح تضمین پایین تر (یعنی PAL2) نسبت به گواه مکانیکی در این استاندارد ملی مورد توجه قرار می‌گیرد. PAL2 به صورت کلی تنها برای پروتکل‌های ساده در محیط شبکه باز مانند اینترنت موثر است.

در PAL3، طراح پروتکل، یک مشخصه پروتکل را در یک زبان مشخصه ویژه ابزار رسمی‌ارائه می‌دهد. بنابراین طراح می‌تواند تمام ردیابی‌های سازگار با مشخصه در محدوده مشخص شده برای تصدیق را کنترل کند. طراحان نوعا در پیش بینی تمام ردیابی‌های (جاگذاری شده) ممکن ضعیف هستند و از این رو این ردیابی‌ها معمولا شامل ردیابی‌های پیچیده که به وسیله طراح پروتکل از پیش مدنظر قرار نمی‌گیرد خواهد بود. PAL3 به صورت کلی ضمانت‌های منطقی را ارائه می‌دهد که هیچ مخالف موفق دیگری در محدوده‌ای از تعداد دوره‌های پروتکل وجود ندارد. PAL3 می‌تواند برای محیط شبکه باز توصیه شود.

تفاوت میان PAL3 و PAL4 این است که آیا تحلیل (و از این رو گواه ارائه شده) برای تصدیق نامحدود است و یا خیر. تصدیق در PAL3، محدود است و از این رو طراح نمی‌تواند امنیت پروتکل خود را برای حملات پیچیده که خارج از محدوده قرار دارند اثبات کند. در مقابل، PAL3، ضمانت‌های قدرتمندی درمورد اینکه هیچ مخالف (نمادین، Dolev-Yao) موفقی، حتی پذیرفته شده برای تعداد نامحدود دوره‌ها، وجود ندارد را می‌دهد. با تصدیق نامحدود، یک طراح پروتکل می‌تواند امنیت پروتکل خود را در مقابل تمام مخالفان، حتی مواردی که خواستار اجرای حملات پیچیده و پرهزینه هستند، اثبات کند. PAL4 برای سامانه‌های اطلاعاتی حساس، مانند مواردی که زیرساخت‌های اجتماعی یا سامانه‌های اقتصادی را فراهم می‌کنند، کارآمد است.

۶-۷سطوح تضمین متشابه در ISO/IEC 15408

هدف از این استاندارد ملی مشخص کردن روش سنجیدن امنیت پروتکل‌های رمزنگاشتی در یک سطح مشخصه است. اول این‌که باید تاکید شود که این استاندارد حتی در سنجیدن پروتکل‌های رمزنگاشتی ویژه مشخصه مستقل از کل سامانه‌ای‌که پروتکل‌ها اجرا می‌شوند سودمند است. دوم این که، این استاندارد ملی به گونه‌ای طراحی شده است که در سنجیدن پروتکل‌های رمزنگاشتی در سامانه‌های فناوری اطلاعات حساس که اغلب هدف گواهی ISO/IEC 15408 هستند، مفید باشد.

یادآوری- درمورد استفاده از این استاندارد ملی به صورت مشترک با ISO/IEC 15408 جهت سنجیدن امنیت کلی سامانه‌های فناوری اطلاعات شامل پروتکل‌های رمزنگاشتی، جدول ۲ مطابقت میان سطوح تضمین سنجش (EAL) را در ISO/IEC 15408 سامانه فناوری اطلاعات و سطوح تضمین پروتکل (PAL) را در این استاندارد ملی نشان می‌دهد. در این مورد، توسعه دهنده باید زیر مجموعه‌ای از پروتکل‌های رمزنگاشتی را در TOE به عنوان مجموعه‌ای از پروتکل‌های هدف جهت سنجیده شدن در این استاندارد ملی شناسایی کند. این مجموعه از پروتکل‌های هدف باید تمام پروتکل‌های رمزنگاشتی حساس را در TOE پوشش دهد. پروتکل‌های رمزنگاشتی که اطلاعات حساس را در یک شبکه باز تبادل می‌کنند یا به عنوان یک زیرساخت اجتماعی مورد استفاده قرار می‌گیرند مثال‌هایی از پروتکل‌های هدف بلندمدت هستند.

جدول ۲ (اطلاعاتی)- مطابقت بررسی شده میان EAL و PAL

ISO/IEC 15408 EAL	ISO/IEC 29128 PAL	
	پروتکل‌های هدف در TOE	دیگر پروتکل‌ها در TOE
EAL 7	PAL4	
EAL 6	PAL 3	
EAL 5		
EAL 4	PAL 2	
EAL 3		
EAL 2	PAL 1	
EAL 1		

۷ تصدیق و ارزیابی امنیتی

۷-۱ مشخصه پروتکل

۷-۱-۱ PPS_SEMIFORMAL

۷-۱-۱-۱ اهداف

مشخصه پروتکل در PPS_SEMIFORMAL باید قسمت‌های مرتبط امنیتی پروتکل را در یک زبان نیمه رسمی، معمولا به عنوان دنباله‌ای از پیام‌های تبادل شده مشخص کند. پیوست ۱، « رهنمودهایی برای طراحی پروتکل رمزنگاشتی» مسائل مرتبط را زمانی که یک طراح پروتکل یک پروتکل را برای PPS_SEMIFORAML طراحی می‌کند یا می‌سنجد را توضیح می**دهد**. یک طراح پروتکل باید این مسائل را در طراحی مشخصه پروتکل ایمن مدنظر قرار دهد.

۷-۱-۱-۲ عناصر عمل توسعه دهنده

توسعه دهنده مشخصه پروتکل رمزنگاشتی هدف که به زبان نیمه رسمی‌نوشته شده است را ارائه می‌دهد.

۷-۱-۱-۳عناصر ارائه و محتوا

مشخصه پروتکل باید دنباله‌های پروتکل را که شامل عملیات اجرا شده توسط تمام مشترکان پروتکل، اطلاعات مورد نیاز این عملیات رمزنگاشتی و پیام پروتکل می‌شود را شرح دهد.

۷-۱-۱-۴ عناصر عمل ارزیاب (سنجش‌گر)

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات محتوا و ارائه را برآورده می‌کند.

۷-۱-۲ PP_FORMAL

۷-۱-۲-۱ اهداف

مشخصه پروتکل در PPS_FORMAL باید قسمت‌های مرتبط امنیتی پروتکل را به یک زبان رسمی‌مشخص کند. نحوهای زبانی باید به طور صریح یا ضمنی تعریف شود.

۷-۱-۲-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید PPS_SEMIFORMAL و مشخصه پروتکل رمزنگاشتی هدف که به یک زبان رسمی‌نوشته می‌شود را ارائه دهد.

۷-۱-۲-۳ عناصر ارائه و محتوا

مشخصه پروتکل رسمی‌باید تمام موارد لازم در بند ۵-۳ مانند پیام‌ها، پیام‌های مشاهده‌ای[1]، ویژگی‌های جبری و نقش‌های پروتکل که به یک زبان رسمی‌نوشته شده است را شرح دهد. این مشخصه پروتکل رسمی‌باید با PPS_SEMIFORAML مطابقت کند.

۷-۱-۲-۴عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

۷-۱-۳ PPS_MECHANIZED

۷-۱-۳-۱ اهداف

مشخصه پروتکل در PPS_MECHANIZED باید قسمت‌های مرتبط با امنیت پروتکل را به زبان مشخصه ویژه ابزار رسمی‌مشخص کند.

یادآوری۱- پروتکل‌ها می‌توانند به یک زبان مشخصه ویژه ابزار به صورت نمایش خودکار پروتکل (مانند Mealy Machines) برای اصول مختلف مشخص شوند و یا به صورت یک نشان گذاری ثابت[4] ، که در آن یک مورد برای هر نقش، پیام‌های ارسال شده و دریافت شده فهرست می‌شود، مشخص می‌شود.

یادآوری ۲- پروتکل‌ها می‌توانند به یک زبان منطقی گزاره‌ای کلی به صورت یک مجموعه به صورت استنتاجی تعریف شده مشخص شوند که مجموعه عمل‌های امکان پذیر (برای مثال رویدادهای ارتباطی) ناشی شده از اصول دنبال کننده نقش‌های پروتکل آنها و همچنین یک متجاوز را به صورت رسمی‌بیان می‌کند. پروتکل‌ها نیز می‌توانند با نشان گذاری مبتنی بر فرآیندها، سامانه‌های انتقال یا کرانه‌ها (strands) مشخص شوند که رسمی‌سازی می‌تواند برحسب عمل‌های رسمی‌اصول مختلف (برای مثال فرآیندهای منفرد آنها یا سامانه‌های انتقال محلی) یا سامانه انتقال کلی باشد.

۷-۱-۳-۲عناصر عمل توسعه دهنده

توسعه دهنده باید PPS_SEMIFORMAL را ارائه دهد.

توسعه دهنده باید مشخصه‌ای از پروتکل رمزنگاشتی هدف را که به یک زبان مشخصه ویژه ابزار نوشته شده را ارائه دهد.

توسعه دهنده باید اطلاعات درمورد زبانی که شرح مشخصه پروتکل هدف را مورد استفاده قرار می‌دهد را ارائه دهد.

۷-۱-۳-۳ عناصر محتوا و ارائه

مشخصه پروتکل رسمی‌باید تمام موارد ضروری در بند ۵-۳ مانند پیام‌ها، پیام‌های مشاهده‌ای، ویژگی‌های جبری و نقش‌های پروتکل که به زبان مشخصه ویژه ابزار رسمی‌نوشته شده است را شرح دهد. این مشخصه پروتکل رسمی‌باید مطابق با PPS_SEMIFORMAL باشد. اطلاعات درمورد زبان مشخصه ویژه ابزار باید شامل موادی مانند راهنماها و اوراق مرجع باشد.

۷-۱-۳-۴عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

1- observing

۷-۲مدل مخالف

۷-۲-۱ PAM_INFORAML

۷-۲-۱-۱ اهداف

مدل مخالف برای PAM_INFORMAL باید مدل متجاوز، ویژگی‌های مجرای ارتباطی و سناریو را نوعا به یک زبان غیررسمی‌مشخص کند.

۷-۲-۱-۲عناصر عمل توسعه دهنده

توسعه دهنده باید توضیحی در مورد مدل مخالف را ارائه دهد.

۷-۲-۱-۳ عناصر محتوا و ارائه

توضیح مدل مخالف باید تمام موارد لازم در بند ۵-۴ را از جمله مشخصه، توانایی مهاجم و سناریو شرح دهد.

۷-۲-۱-۴عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کنند.

۷-۲-۲ RAM_FORMAL

۷-۲-۲-۱ اهداف

مدل مخالف برای PAM_FORMAL باید مدل متجاوز و ویژگی‌های مجرای ارتباطی را در یک زبان رسمی‌مشخص کند. نحوهای زبان باید به صورت صریح یا ضمنی تعریف شود. که می‌تواند مهاجم Dolev-Yao [3] یا گزینه‌ای وابسته به آن باشد. مدل مهاجم Dolev-Yao یک نمونه از محیط عملیاتی است که تحت کنترل کامل مهاجم است، یعنی، هر پیام در شبکه می‌تواند دانسته شود، تحریف شود و توسط مهاجم ایجاد شود. متغیرها ممکن است شامل مهاجم‌های ضعیف تر مانند مهاجم منفعل باشد که تنها می‌تواند در شبکه استراق سمع کند یا یک مهاجم بی سیم که هم می‌تواند استراق سمع کند و هر پیامی‌را ایجاد کند، اما نمی‌تواند پیامی را با دانستن پیام منحرف کند. متغیرها ممکن است زمانی که ویژگی‌های افزوده طرح ریزی شده عامل‌های رمزنگاشتی هستند (برای مثال، ویژگی‌های جبری [1,2]) نیز به وجود آیند.

۷-۲-۲-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید PAM_INFORMAL را ارائه دهد.

توسعه دهنده باید توضیح مدل مخالف را به یک زبان رسمی‌ارائه دهد.

۷-۲-۲-۳ عناصر محتوا و ارائه

توضیح مدل مخالف باید تمام موارد لازم در بند ۵-۴ مانند مشخصه شبکه، توانایی مهاجم و سناریو نوشته شده به زبان رسمی‌را شرح دهد. این مدل مخالف رسمی‌باید با PAM_INFORMAL مطابقت داشته باشد.

۷-۲-۲-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

۷-۲-۳ PAM_MECHANIZED

۷-۲-۳-۱ اهداف

مدل مخالف برای PAM_MECHANIZED باید مدل متجاوز و ویژگی‌های مجرای ارتباطی به یک زبان رسمی‌مشخصه ویژه ابزار را مشخص کند. می‌تواند متجاوز Dolev-Yao [3] یا متغیری وابسته به آن باشد. مدل

متجاوز Dolev-Yao نمونه‌ای از محیط عملیاتی است که در آن شبکه تحت کنترل کامل متجاوز است، یعنی هر پیام به وسیله متجاوز می‌تواند در شبکه دانسته، تحریف و ایجاد شود. متغیرهای ممکن است شامل متجاوزان ضعیف‌تر مانند متجاوز منفعل باشد که تنها می‌تواند در شبکه استراق سمع کند یا یک متجاوز بی سیم که می‌تواند هم استراق سمع کند و هر پیامی را ارسال کند، اما نمی‌تواند پیامی‌را با دانستن پیام منحرف کند. متغیرها نیز می‌توانند زمانی که ویژگی‌های افزوده طرح ریزی عامل‌های رمزنگاشتی هستند (برای مثال ویژگی‌های جبری [1,2]) ایجاد شوند.

۷-۲-۳-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید PAM_INFORMAL را ارائه دهد.

توسعه دهنده باید توضیحی درمورد مدل مخالف به زبان مشخصه ویژه ابزار ارائه دهد.

توسعه دهنده باید اطلاعات درمورد زبانی که جهت شرح مدل مخالف پروتکل هدف مورد استفاده قرار می‌دهد را ارائه دهد.

۷-۲-۳-۳ عناصر محتوا و ارائه

توضیح مدل مخالف باید تمام موارد لازم در بند ۵-۴، مانند مشخصه شبکه، توانایی مهاجم و سناریو نوشته شده به یک زبان مشخصه ویژه ابزار رسمی‌را شرح دهد. این مدل مخالف رسمی‌باید با PAM_INFORMAL مطابقت داشته باشد.

اطلاعات در مورد زبان مشخصه ویژه ابزار باید شامل موادی مانند دستورالعمل‌های مرجع و اوراق باشد.

۷-۲-۳-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

یادآوری ۱- مدل مخالف می‌تواند به زبان مشخصه ویژه ابزار مشخص شود. به دلایل بهره وری، بیشتر ابزارها این مدل متجاوز را در ابزارهایشان «سیم بسته» می‌کنند، برای مثال از طریق calculi اختصاصی برای حل محدودیت‌ها. درصورتی که یک مورد از بازبین مدل هدف کلی استفاده کند، یک مورد باید صریحا متجاوز را به عنوان یک فرآیند نشان دهد.

یادآوری ۲- مدل مخالف می‌تواند به یک زبان منطقی گزاره‌ای کلی به عنوان یک مجموعه به صورت قیاسی تعریف شده به عنوان قسمتی از مشخصه پروتکل مشخص شود. مدل مخالف می‌تواند به عنوان رسمی‌سازی متجاوز که در ابزارهای تصدیق گنجانده شده است مشخص شود.

۷-۳ ویژگی‌های امنیتی

۷-۳-۱ کلیات

ویژگی‌های φ الزامات درمورد رفتار پروتکل را مشخص می‌کند. برای اکثریت روش‌های رسمی، مدل M یک سامانه تراکنش را تشکیل می‌دهد که وضعیت‌های سامانه و تراکنش‌های میان وضعیت‌ها را شرح می‌دهد. در این برقرارسازی، یک ویژگی φ نوعا یا یک ویژگی وضعیت است، یعنی نامتغیری که باید برای تمام وضعیت‌های سامانه قابل دسترسی برقرار باشد یا یک ویژگی موقتی شرح دهنده دنباله‌های معتبر وضعیت‌ها (یا رویدادهای سامانه) است. یک ویژگی محرمانه بودن (یا قابلیت اطمینان) به طور کلی نامتغیر یک وضعیت است و بیان می‌کند که مجموعه S موارد داده (برای مثال کلیدها و واژه‌ها) هرگز به وسیله مهاجم در یک شکل رمزنگاشتی نشده بدست نخواهد آمد. ویژگی‌های تصدیق هم شامل تصدیق ریشه پیام (که یک پیام به طور فرضی از سوی

گروهی فرستاده شده است در واقع از سوی آن قسمت فرستاده شده است) و هم تصدیق نهاد می‌شود (به طور کلی اینکه یک اصل معین درحال حاضر در قسمتی از نقش بیان شده دخالت دارد).

۷-۳-۲ PSP_INFORMAL

۷-۳-۲-۱ اهداف

ویژگی‌های امنیتی برای PSP_INFORMAL باید مشخصه غیر رسمی‌ویژگی‌های امنیتی را به یک زبان غیر رسمی‌مشخص کند.

۷-۳-۲-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید توضیحی درمورد ویژگی امنیتی که پروتکل باید بدست آورد، ارائه دهد.

۷-۳-۲-۳ عناصر محتوا و ارائه

توضیح درمورد ویژگی امنیتی باید تمام ویژگی‌هایی که پروتکل باید بدست آورد را تحت پوشش قرار دهد.

۷-۳-۲-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

۷-۳-۳ PSP_FORMAL

۷-۳-۳-۱اهداف

ویژگی‌های امنیتی برای PSP_FORMAL باید الزامات درمورد رفتار پروتکل به یک زبان رسمی‌را مشخص کند. نحوهای زبان باید به صورت دقیق یا مفهومی‌تعریف کند.

۷-۳-۳-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید PSP_INFORMAL را ارائه کند.

توسعه دهنده باید توضیحی را در مورد ویژگی امنیتی که پروتکل باید بدست آورد را فراهم کند. این امر باید به زبان رسمی‌نوشته شود.

۷-۳-۳-۳ عناصر محتوا و ارائه

توضیح درمورد ویژگی امنیتی این که تمام ویژگی‌هایی که پروتکل باید بدست آورد که به یک زبان رسمی‌نوشته شده است را به روشی که در بند ۵-۵ شرح داده شده است، پوشش دهد. این ویژگی امنیتی رسمی‌باید با PSP_INFORMAL مطابقت کند.

۷-۳-۳-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

۷-۳-۴ PSP_MECHANIZED

۷-۳-۴-۱ اهداف

ویژگی‌های امنیتی برای PSP_MECHANIZED باید الزامات درمورد رفتار پروتکل را به یک زبان مشخصه ویژه ابزار رسمی‌مشخص کند.

۷-۳-۴-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید PSP_INFORMAL را ارائه دهد.

توسعه دهنده باید توضیحی درمورد ویژگی امنیتی که پروتکل باید بدست آورد را ارائه دهد. این توضیح باید به زبان مشخصه ویژه ابزار رسمی‌نوشته شود.
توسعه دهند باید اطلاعات درمورد زبانی که باید برای شرح ویژگی‌های امنیتی پروتکل هدف مورد استفاده قرار می‌گیرد را ارائه دهد.

۷-۳-۴-۳عناصر محتوا و ارائه

توضیح درمورد ویژگی امنیتی باید تمام ویژگی‌هایی که پروتکل باید بدست آورد که به یک زبان رسمی‌مشخصه ویژه ابزار به روشی که در بند ۵-۵ نوشته شده است را پوشش می‌دهد. این ویژگی امنیتی رسمی باید با PSP_INFORMAL مطابقت کند.
اطلاعات درموردد زبان مشخصه ویژه ابزار باید شامل موادی مانند دستورالعمل مرجع و اوراق باشد.

۷-۳-۴-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات محتوا و ارائه را برآورده می‌کند.

یادآوری- ابزارهای تصدیق مانند جدیدترین نمونه نشان گذارهای مدل مجموعه‌ای از گزاره‌های از پیش تعیین شده را جهت رسمی‌سازی ویژگی‌های امنیتی نمونه مانند محرمانه بودن و نشانه‌های گوناگون تصدیق، ارائه می‌دهد. از این رو، با چنین ابزارهای تصدیق، مشخصه ویژگی امنیتی شامل انتخاب و معرفی گزاره‌های امنیتی مناسب، برای مثال، نشان دادن اینکه کدام اصطلاحات باید محرمانه باقی بمانند، یا اینکه کدام مقادیر باید با کدام اصول مورد قبول واقع شوند، می‌شود.

۷-۴ گواه خود ارزیابی برای تصدیق

۷-۴-۱ کلیات

گواه خود ارزیابی تصدیق، گواهی این است که طراح پروتکل مسئله نشان گذاری مدل، نشان دهنده اینکه مدل M دارای ویژگی φ است را حل می‌کند، یعنی M، φ را جبران می‌کند. تنوعی در روش‌های رسمی‌دارای صلاحیت برقراری یا رد اینکه M، φ را جبران می‌کند وجود دارد.

۷-۴-۲ PEV_ARGUMENT

۷-۴-۲-۱ اهداف

گواه تصدیق PEV_ARGUMENT شامل نشانوند غیررسمی‌برای اینکه چرا پروتکل دارای ویژگی‌های مشخص شده است می‌شود.

۷-۴-۲-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید اطلاعات درمورد اینکه چگونه مشخصه پروتکل ویژگی امنیتی در مدل مخالف را تامین می‌کند را ارائه دهد.

۷-۴-۲-۳ عناصر محتوا و ارائه

اطلاعات باید به روشی قابل تصدیق دلیل اینکه چرا مشخصه پروتکل ویژگی امنیتی را در مدل مخالف تضمین می‌کند را شرح دهد.

۷-۴-۲-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای ارائه و محتوا را برآورده می‌کند.

۷-۴-۳ PEV_HANDPROVEN

۷-۴-۳-۱ اهداف

گواه تصدیق برای PEV_HANDPROVEN شامل گواه به صورت ریاضی رسمی‌کاغذ و قلم درمورد اینکه چرا پروتکل دارای ویژگی‌های مشخص شده است می‌باشد.

۷-۴-۳-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید اطلاعات درمورد اینکه چگونه مشخصه پروتکل ویژگی امنیتی در مدل مخالف را انجام **می‌دهد را ارائه دهد.**

۷-۴-۳-۳ عناصر محتوا و ارائه

اطلاعات باید به روشی قابل تصدیق دلیل اینکه چرا مشخصه پروتکل ویژگی امنیتی را در مدل مخالف تضمین می‌کند را شرح دهد.

۷-۴-۳-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

۷-۴-۴ PEV_BOUNDED

۷-۴-۴-۱ اهداف

گواه تصدیق برای PEV_BOUNDED شامل مشخصه پروتکل و ویژگی‌های امنیتی و (درصورت لزوم) مدل مخالف مورد استفاده به وسیله یک ابزار تصدیق مانند نشان گذارهای مدل همراه با عوامل افزوده می‌شود. مهمترین عامل ارائه یک محدوده در تعداد مثال‌های نقش است. نشان گذارهای مدل مختلف روش‌های مختلف انجام این کار را ارائه می‌دهند. گواه ورودی برای ابزار است. درصورتی که یک پروتکل ویژگی‌های معرفی شده را برآورده کند، ابزارهای به سادگی این مسئله را گزارش می‌دهد. درصورتی که پروتکل نتواند ویژگی‌ها را برآورده کند، ابزارها باید خروجی اطلاعاتی مانند یک جدول دنباله پیام یا ردیاب را ارائه دهند.

۷-۴-۴ -۲ عناصر عمل توسعه دهنده

توسعه دهنده باید گواهی درمورد چگونگی اینکه مشخصه پروتکل PPS_MECHANIZED ویژگی امنیتی PSP_MECHANIZED را در مدل مخالف PAM_MECHANIZED برای تعداد محدودی از مثال‌های نقش برآورده می‌کند را ارائه می‌دهد.

توسعه دهنده باید توضیحی درمورد اینکه ابزار تصدیق مورد استفاده درست است ارائه دهد.

۷-۴-۴-۳ عناصر محتوا و ارائه

گواه باید نتایج ابزار تصدیق را به روشی که قابل تکرار هستند شرح دهد. گواه باید به روشنی مشخص کند که تعداد مثال‌های نقشی که با آنها امنیت پروتکل تضمین می‌شود را مشخص کند.

توضیح باید صحت ابزار تصدیق مورد استفاده و درستی دلیل را شرح دهد.

۷-۴-۴-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

۷-۴-۵ PEV_UNBOUNDED

۷-۴-۵-۱ اهداف

گواه برای تصدیق PEV_UNBOUNDED گواهی است که طراح پروتکل مسئله نشان گذاری مدل نشان دهنده اینکه مدل M دارای ویژگی φ برای تعداد نامحدودی از مثال‌های نقش یک درمیان است را حل می‌کند.

این گواه باید با کمک یک ابزار تصدیق ساخته شود. گواه مورد نیاز برای تصدیق به ابزار تصدیق وابسته است. طراحان پروتکل می‌توانند جدیدترین نمونه‌های ابزار تصدیق مانند اثبات کننده نظریه و نشان گذارهای مدل را انتخاب کنند. اثبات کننده‌های نظریه برای اولین یا بالاترین مرتبه منطق، معمولا به عنوان ورودی یک فایل آغازگر[1] فرمان‌ها درنظر گرفته می‌شوند. دلایل از قواعد یا فنون استنباط ساخته می‌شود، که برنامه‌هایی هستند که دلایل را شکل می‌دهند. در فرآیند تصدیق، فایل آغازگر ورودی برای اثبات کننده نظریه است. درصورتی که هریک از فرمان‌ها خراب شود، تصدیق نیز خراب می‌شود. در صورتی که فایل آغازگر، دلیل با موفقیت اجرا شود، تمام نظریات بیان شده در فایل آغازگر و از این رو درمورد پروتکل اثبات شده، معتبر است.

اعتبار نتایج نهایی به درستی منطق مورد استفاده، به‌کارگیری صحیح در اثبات کننده نظریه و اینکه تمام بسط‌های صورت گرفته در مورد منطق (با افزایش تعاریف، قواعد، غیره) که به روشی صورت گرفته است که سازگاری منطق را حفظ می‌کند، بستگی دارد. طراحان پروتکل باید اطلاعات مربوط به اعتبار نتایج را ارائه دهند.

۷-۴-۵-۲ عناصر عمل توسعه دهنده

توسعه دهنده باید دلیلی درمورد اینکه چگونه مشخصه پروتکل PPS_MECHANIZED ویژگی امنیتی PSP_MECHANIZED را در مدل مخالف PAM_MECHANIZED برای تعداد نامحدودی از مثال‌های نقش برآورده می‌کند را مقرر کند.

توسعه دهنده باید توضیحی درمورد اینکه ابزار تصدیق مورد استفاده درست است را ارائه دهد.

۷-۴-۵-۳ عناصر محتوا و ارائه

دلیل باید نتایج ابزار تصدیق را به روشی که قابل تکرار هستند را شرح می‌دهد.

دلیل باید نشان دهد که امنیت پروتکل با تعداد نامحدود مثال‌های نقش تضمین می‌شود.

توضیح باید صحت ابزار تصدیق مورد استفاده و درستی دلیل را شرح دهد.

۷-۴-۵-۴ عناصر عمل ارزیاب

ارزیاب باید تصدیق کند که اطلاعات ارائه شده تمام الزامات برای محتوا و ارائه را برآورده می‌کند.

۸ روش متداول برای ارزیابی امنیت پروتکل‌های رمزنگاشتی

۸-۱ مقدمه

این بند روش‌های متداول برای ارزیابی پروتکل رمزنگاشتی را مطابق با این استاندارد ملی نشان می‌دهد.

1- Script

۸-۲ ارزیابی مشخصه پروتکل

۸-۲-۱ ارزیابی فعالیت فرعی (PPS_SEMIFORMAL)

۸-۲-۱-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- مشخصه پروتکل رمزنگاشتی هدف نوشته شده به زبان نیمه رسمی.

۸-۲-۱-۲ عمل

ارزیاب باید تصدیق کند که مشخصه پروتکل رسمی، دنباله‌های پروتکل که شامل عملیات رمزنگاشتی اجرا شده به وسیله تمام مشترکان پروتکل، اطلاعات مورد نیاز این عملیات رمزنگاشتی و پیام پروتکل می‌شود را شرح **می‌دهد.**

۸-۲-۲ ارزیابی فعالیت فرعی (PPS_FORMAL)

۸-۲-۲-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

PPS_SEMIFORMAL-

-مشخصه پروتکل رمزنگاشتی هدف نوشته شده به زبان رسمی

۸-۲-۲-۲ عمل

ارزیاب باید تصدیق کند که مشخصه پروتکل رسمی‌تمام موارد لازم در بند ۵-۳ مانند پیام‌ها، پیام‌های مشاهده‌ای، ویژگی‌های جبری و قوانین پروتکل نوشته شده به زبان رسمی‌را شرح می‌دهد.

ارزیاب باید تصدیق کند که این مشخصه پروتکل رسمی‌با PPS_SEMIFORMAL مطابقت می‌کند.

۸-۲-۳ ارزیابی فعالیت فرعی (PPS_MECHANIZED)

۸-۲-۳-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

PPS_SEMIFORMAL-

- مشخصه پروتکل رمزنگاشتی هدف نوشته شده به زبان مشخصه ویژه ابزار رسمی.
- اطلاعات در مورد زبانی که برای شرح مشخصه پروتکل هدف.

۸-۲-۳-۲ عمل

ارزیاب باید تصدیق کند که مشخصه پروتکل رسمی‌تمام موارد لازم در بند ۵-۳ را مانند پیام‌ها، پیام‌های مشاهده‌ای، ویژگی‌های جبری و قواعد پروتکل نوشته شده به زبان مشخصه ویژه ابزار رسمی را شرح می‌دهد.

ارزیاب باید تصدیق کند که این مشخصه پروتکل رسمی‌با PPS_SEMIFORMAL مطابقت می‌کند.

ارزیاب باید تصدیق کند که اطلاعات درمورد زبان مشخصه ویژه ابزار شامل موادی مانند دستورالعمل‌های مرجع و اوراق می‌شود.

۸-۳ ارزیابی مدل مخالف

۸-۳-۱ ارزیابی فعالیت فرعی (PAM_INFORAML)

۸-۳-۱-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- توضیح درمورد مدل مخالف

۸-۳-۱-۲ عمل

ارزیاب باید تصدیق کند که توضیح مدل مخالف تمام موارد لازم در بند ۵-۴ مانند مشخصه شبکه، توانایی مهاجم و سناریو را شرح می‌دهد.

۸-۳-۲ ارزیابی فعالیت فرعی (PAM_FORMAL)

۸-۳-۲-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- PAM_INFORMAL
- توضیح مدل مخالف به زبان رسمی.

۸-۳-۲-۲ عمل

ارزیاب باید تصدیق کند که توضیح مدل مخالف تمام موارد لازم در بند ۵-۴ مانند مشخصه شبکه، توانایی مهاجم و سناریو نوشته شده به زبان رسمی‌را شرح می‌دهد.

ارزیاب باید تصدیق کند که این مدل مخالف رسمی‌با PAM_INFORMAL مطابقت دارد.

۸-۳-۳ ارزیابی فعالیت فرعی (PAM_MECHANIZED)

۸-۳-۳-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- PAM_INFORMAL
- توضیح مدل مخالف به یک زبان مشخصه ویژه ابزار رسمی.
- اطلاعات درمورد زبانی که که جهت شرح مدل مخالف پروتکل هدف مورد استفاده قرار می‌گیرد.

۸-۳-۳-۲ عمل

ارزیاب باید تصدیق کند که توضیح مدل مخالف تمام موارد لازم در بند ۵-۴ مانند مشخصه شبکه، توانایی مهاجم و سناریو نوشته شده به زبان مشخصه ویژه ابزار رسمی‌را شرح می‌دهد.

ارزیاب باید تصدیق کند که این مدل مخالف رسمی‌با PAM_INFORMAL مطابقت دارد.

ارزیاب باید تصدیق کند که اطلاعات درمورد زبان مشخصه ویژه ابزار شامل موادی مانند دستورالعمل مرجع و اوراق می‌شود.

۸-۴ ارزیابی ویژگی‌های امنیتی

۸-۴-۱ ارزیابی فعالیت فرعی (PSP_INFORMAL)

۸-۴-۱-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- توضیح درمورد ویژگی امنیتی که پروتکل باید به آن دست یابد.

۸-۴-۱-۲ عمل

ارزیاب باید تصدیق کند که توضیح درمورد ویژگی امنیتی تمام ویژگی‌هایی که پروتکل باید به آنها دست یابد را پوشش می‌دهد.

۸-۴-۲ ارزیابی فعالیت فرعی (PSP_FORMAL)

۸-۴-۲-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- PSP_INFORMAL
- توضیح درمورد ویژگی امنیتی که پروتکل باید به آنها دست یابد. این توضیح باید به زبانی رسمی‌نوشته شود.

۸-۴-۲-۲ عمل

ارزیاب باید تصدیق کند که توضیح درمورد ویژگی امنیتی تمام ویژگی‌هایی که پروتکل باید به آنها دست یابد که به زبان رسمی‌به روشی که در بند ۵,۵ شرح داده شده است را پوشش دهد.

ارزیاب باید تصدیق کند که این ویژگی امنیتی رسمی‌با PSP_INFORMAL مطابقت می‌کند.

۸-۴-۳ ارزیابی فعالیت فرعی (PSP_MECHANIZED)

۸-۴-۳-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

PSP_INFORMAL

- توضیح درمورد ویژگی امنیتی که پروتکل باید به آن دست یابد. این توضیح باید به یک زبان مشخصه ویژه ابزار رسمی‌نوشته شود.
- اطلاعات درمورد زبانی که جهت شرح ویژگی‌های امنیتی پروتکل هدف مورد استفاده قرار گرفته است.

۸-۴-۳-۲ عمل

ارزیاب باید تصدیق کند که توضیح درمورد ویژگی امنیتی تمام ویژگی‌هایی که پروتکل باید به آنها دست یابد که به زبان مشخصه ویژه ابزار رسمی‌به روشی که در بند ۵-۵ شرح داده شده است را پوشش دهد.

ارزیاب باید تصدیق کند که این ویژگی امنیتی رسمی‌با PSP_INFORMAL مطابقت می‌کند.

ارزیاب باید تصدیق کند که اطلاعات درمورد زبان مشخصه ویژه ابزار شامل موادی مانند دستورالعمل مرجع و اوراق می‌شود.

۸-۵ ارزیابی شواهد خودارزیابی

۸-۵-۱ ارزیابی فعالیت فرعی (PEV_ARGUMENT)

۸-۵-۱-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- اطلاعات درمورد چگونگی برآورده شده

ویژگی امنیتی در مدل مخالف از سوی مشخصه پروتکل

۸-۵-۱-۲ عمل

ارزیاب باید تصدیق کند که اطلاعات دلیل را به روشی قابل تصدیق در مورد اینکه چرا مشخصه پروتکل ویژگی امنیتی را در مدل مخالف تضمین می‌کند، شرح می‌دهد.

۸-۵-۲ ارزیابی فعالیت فرعی (PEV_HANDPROVEN)

۸-۵-۲-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- مدرک کاغذ و قلم به صورت ریاضی

رسمی‌درمورد اینکه چگونه مشخصه پروتکل ویژگی امنیتی را در مدل مخالف برآورده می‌کند.

۸-۵-۲-۲ عمل

ارزیاب باید تصدیق کند که اطلاعات دلیل را به روشی قابل تصدیق در مورد اینکه چرا مشخصه پروتکل ویژگی امنیتی را در مدل مخالف تضمین می‌کند، شرح می‌دهد.

۸-۵-۳ ارزیابی فعالیت فرعی (PEV_BOUNDED)

۸-۵-۳-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

دلیل اینکه چگونه مشخصه پروتکل PPS_MECHANIZED ویژگی امنیتی PSP_MECHANIZED را در مدل مخالف PAM_MECHANIZED برای تعداد محدودی از مثال‌های نقش برآورده می‌کند.

توضیح درمورد اینکه ابزار تصدیق مورد استفاده درست است.

۸-۵-۳-۲عمل

ارزیاب باید تصدیق کند که دلیل نتایج ابزار تصدیق را به روشی شرح می‌دهد که قابل تکرار هستند.

ارزیاب باید تصدیق کند که دلیل به روشنی، تعداد مثال‌های نقشی را که با آنها امنیت پروتکل تضمین می‌شود را مشخص می‌کند.

ارزیاب باید تصدیق کند که توضیح صحت ابزار تصدیق مورد استفاده و درستی دلیل را شرح می‌دهد.

۸-۵-۴ ارزیابی فعالیت فرعی (PEV_UNBOUNDED)

۸-۵-۴-۱ ورودی

گواه ارزیابی برای این فعالیت فرعی به صورت زیر است:

- دلیل درمورد اینکه چگونه مشخصه پروتکل PPS_MECHANIZED ویژگی امنیتی PSP_MECHANIZED در مدل مخالف PAM_MECHANIZED را برای تعداد نامحدود مثال‌های نقش برآورده می‌کند.
- توضیح اینکه ابزار تصدیق مورد استفاده درست است.

۸-۵-۴-۲ عمل

ارزیاب باید تصدیق کند که دلیل نتایج ابزار تصدیق را به روشی شرح می‌دهد که قابل تکرار هستند.

ارزیاب باید تصدیق کند که دلیل نشان می‌دهد که امنیت پروتکل با تعداد نامحدود مثال‌های نقش تضمین شده است.

ارزیاب باید تصدیق کند که توضیح صحت ابزار تصدیق مورد استفاده و درستی دلیل را شرح می‌دهد.

پیوست الف

(اطلاعاتی)
رهنمودهایی برای طراحی پروتکل رمزنگاشتی

این پیوست اطلاعاتی رهنمودهای شناخته شده‌ای را برای طراحی پروتکل‌های رمزنگاشتی ارائه می‌دهد. این رهنمودها به طراح پروتکل رمزنگاشتی کمک می‌کند تا از خطاهای نوعی جلوگیری کند. باید توجه داشت که یک پروتکل طراحی شده همراه با اصول لزوما با این استاندارد ملی مطابق نیست. پروتکل طراحی شده باید به صورت جداگانه برای مطابقت داشتن تصدیق شود.

این بند رهنمودهای طراحی در [5] را ارائه می‌دهد. رهنمودهای مشابهی نیز در [6] ارائه شده‌اند.

۱ هر پیام باید بیان کند آنچه که تفسیر پیام معنا می‌دهد باید تنها به محتوای آن وابسته باشد. باید نوشتن یک جمله انگلیسی آسان که محتوا را شرح می‌دهد ممکن باشد- اگرچه درصورتی که رسمی‌سازی مناسب نیز در دسترس باشد مفید خواهد بود.

۲ شرایط برای اینکه یک پیام مبتنی بر واقعیت شود باید به روشی بیان شود تا فردی که طراحی را مورد بررسی قرار می‌دهد بتواند قابل قبول بودن یا نبودن آن را مشاهده کند.

۳ درصورتی که هویت یک عامل[1] برای معنای یک پیام ضروری باشد، ذکر نام عامل به صورت واضح در پیام با احتیاط صورت می‌گیرد.

۴ دلیل اینکه چرا رمزنگاشتی انجام شده است باید روشن باشد. رمزنگاشتی کاملا بی‌ارزش نیست و پرسش نکردن با صراحت دلیل انجام آن می‌تواند به حشو منجر شود. رمزنگاشتی با امنیت مترادف نیست و استفاده نامناسب از آن می‌تواند به خطا منجر شود.

۵ زمانی که عامل موادی را امضا می‌کند که پیش از آن رمزنگاشتی شده‌اند نباید استنباط شود که عامل محتوای پیام را می‌داند. از سوی دیگر استنباط اینکه عاملی که پیامی‌را امضا کرده است و سپس آن را برای حریم شخصی رمزنگاشتی کرده است، محتوای پیام را می‌داند، درست است.

۶ ویژگی‌هایی که درمورد واژه‌ها فرض می‌شوند باید روشن باشند. آنچه که ممکن است برای تضمین توالی موقتی انجام شود ممکن است برای تضمین پیوستگی صورت نگیرد و شاید پیوستگی با ابزارهای دیگر به بهترین نحو برقرار شود.

۷ استفاده از کمیت قابل پیش بینی مانند مقدار یک شمارش‌گر می‌تواند از طریق تبادل چالش- واکنش در ضمانت تازگی به‌کار رود. اما درصورتی که کمیت قابل پیش بینی باید موثر باشد، باید محافظت شود، از این رو یک متجاوز نمی‌تواند چالشی را شبیه سازی کند و پس از آن به واکنش پاسخ دهد.

۸ اگر مقایسه به عنوان حداقل تضمین‌های تازگی با اشاره به زمان مطلق استفاده می شود، تفاوت میان ساعت‌های محلی در ماشین‌های مختلف باید بسیار کمتر از عمر مجاز پیامی معتبر درخواست شده باشد. به علاوه سازوکار حفاظت زمانی در هر جا به قسمتی از مبنای رایانش مورد اطمینان تبدیل می‌شود.

1- principal

۹ کلیدی که می‌تواند به صورت جاری برای مثال جهت رمزنگاشتی یک واژه مورد استفاده قرار گرفته شده باشد درعین حال می‌تواند کاملا قدیمی‌و شاید درخطر باشد. استفاده اخیر از کلید نمی‌تواند آن را بهتر از چیزی نشان دهد که در غیر این صورت خواهد بود.

۱۰ درصورتی که رمزنگاشتی جهت نمایش معنای یک پیام به‌کار رود، باید بیان اینکه کدام رمزنگاشتی مورد استفاده قرار می‌گیرد امکان پذیر باشد. در یک مدل معمول که رمزنگاشتی وابسته به پروتکل است، باید استنباط اینکه پیام به این پروتکل تعلق دارد و در واقع به اجرای ویژه پروتکل و دانستن تعداد آن در پروتکل، ربزیظ ممکن باشد.

۱۱ طراح پروتکل باید بداند که پروتکل وی به کدام روابط مورد اطمینان وابسته است و چرا این وابستگی لازم است. دلایل روابط ویژه مورد اطمینان قابل قبول باید صریح باشند از این رو به جای منطق بر اساس قضاوت و خط مشی شکل خواهند گرفت.

پیوست ب

(اطلاعاتی)
مثال مشخصه رسمی

ب-۱ مشخصه نمادین پروتکل‌های امنیتی

در این قسمت روشی برای مشخصه رسمی پروتکل‌های امنیتی همراه با رهنمودهای ارائه شده در بند ۵ شرح داده می‌شود. اگرچه همچنان تا حد معینی این شرح خلاصه باقی می‌ماند، شرح زیر راه استفاده از روش‌های رسمی‌در تصدیق پروتکل‌ها را نشان می‌دهد. به علاوه، هر گام با یک مثال عینی که از پروتکل کلید عمومیNeedham-Schroeder ساده شده استفاده می‌کند توضیح داده خواهد شد.

سبک شرح ارائه شده از نحو Cas Cremer's Scyther [9] به دلیل استفاده ساده و حسی آن برای مشخصه پروتکل‌های امنیتی، پیروی می‌کند. اگرچه، شرح زیر با مفاهیم پایه Bruno Blanchet's ProVerif [10]، یکی از ابزارهای پیشتاز برای تصدیق نمادین خودکار پروتکل‌های امنیتی نیز مطابقت دارد.

ب-۱-۱ سطح انتزاعی

پروتکل‌ها در مجرد ترین سطح مشخص می‌شوند، یعنی پیام‌ها اصطلاحاتی هستند که از نشانه‌ها ساخته می‌شوند و مهاجم به عنوان یک فرآیند رسمی‌طرح ریزی می‌شود.

ب-۱-۱-۱ زبان‌ها

یک زبان رسمی $\mathcal{L} = (v, \mathcal{C}, \mathcal{R}, \mathcal{F})$ برای پروتکل کلید عمومیNeedham-Schroeder شامل یک مجموعه $\mathcal{V}$ از متغیرها جهت ذخیره پیام‌ها، مجموعه $\mathcal{C}$ از نشانه‌های ثابت محلی برای واژه‌ها، مجموعه $\mathcal{R}$ از نشانه‌های نام نقش، مجموعه $\mathcal{F}$ نشانه‌های عملکرد برای دو عملکرد تولید کلید pk و sk برای تولید کلید عمومی‌یا خصوصی، به ترتیب یک عملکرد جفت سازی دو دویی (۰و۰)، دو عملکرد یکانی π_1 و π_2 جهت تجزیه جفت‌ها، دو عملکرد دودویی enc و dec به ترتیب جهت رمزنگاشتی و رمزگشایی می‌شود.

فرض بر این است که توابع ابتدایی رمزنگاشتی مانند enc و dec کامل هستند. تنها ویژگی‌های مرتبط آنها شناخته شده فرض می‌شوند. هیچ محدودیتی درمورد یک اصطلاح تحمیل نمی‌شود، یعنی تمام اصطلاحاتی که با نشانه‌های عملکرد دنبال کننده محدودیت‌های تعداد نشان‌وندهای ساخته می‌شوند پیام‌های معتبر هستند: یک اصطلاح یک متغیر $v \in \mathcal{V}$، یک واژه $\mathcal{N} \in \mathcal{C}$، نام نقش $r \in R$ یا یک اصطلاح مرکب با استفاده از نشانه عملکرد است.

برخی محدودیت‌ها قابل استفاده هستند که برخی از نشانوندها به برخی از دسته‌ها محدود می‌شوند. در مقابل فرض براین است که اصطلاحات براساس نوع آنها قابل شناسایی هستند: نام‌های نقش، واژه‌ها، کلیدها، رمزنگاشتی، چندتایی‌ها و غیره. یعنی برای مثال، تنها کلیدها می‌توانند جهت رمزنگاشتی یک پیام مورد استفاده قرار گیرند، درغیر این صورت اصطلاحات به صورت مستقیم رد یا از آنها صرف نظر خواهد شد.

ب-۱-۱-۲ ویژگی‌های جبری

درکنار تساوی نحوی اصطلاحات، مشخصه سطح نمادین تساوی پیام شامل معادلات پایه زیر است:

dec(sk(r), enc(pk(r),m)=m

$$\pi_i(m_1, m_2) = m_i i \in \{1,2\}$$

در اینجا بر این نکته اشاره شده است که به صورت کلی، افزودن ویژگی‌های جبری $\oplus$، یا انحصاری، با یک تابع هش[1] هم شکل به مدل مهاجم Dolev-Yao

$(x \oplus y) \oplus z = x \oplus (y \oplus z)$
$x \oplus y = y \oplus x$
$0 \oplus x = x$
$x \oplus 0 = x$
$x \oplus x = 0$

$h(x \oplus y) = h(x) \oplus h(y)$
$\text{enc}(k, x \oplus y) = \text{enc}(k, x) \oplus \text{enc}(k, y)$

فرض رمزنگاشتی بی عیب را تضعیف می‌کند [11].

همچنین براین نکته اشاره شده است که حالت حال حاضر Scyther یا ProVerif نمی‌تواند با یای مانع جمع توافق داشته باشد. از سوی دیگر، تحقیقاتی در مورد چگونگی توافق با یا مانع جمع برای ابزارهای خودکار تصدیق [12] صورت گرفته است.

ب-۱-۲ مشخصات پروتکل

با تعیین یک زبان $\mathcal{L} = (\nu, \mathcal{C}, \mathcal{R}, \mathcal{F})$، یک پروتکل P رفتار هر یک از نقش‌ها مانند آغازگر، پاسخگو، خدمت رسان کلیدی و غیره را شرح می‌دهد. در مشخصه، رفتار هر نقش به عنوان یک سامانه انتقال رسمی‌می‌شود که چگونگی ایجاد پیام، چگونگی واکنش نشان دادن به پیام دریافت شده و چگونگی ویرایش و تغییر دادن آنها را شرح می‌دهد. فرض براین است که تمام ارتباطات از طریق یک مجرای عمومی‌منفرد c صورت می‌گیرد.

ب-۱-۲-۱ ارسال و دریافت رویدادها

از دو نشانه پیش بینی موجود برمبنای سه استفاده می‌شود: Send برای ارسال پیام‌ها و Receive برای دریافت پیام‌ها.

Send (i,r,m) برای i پیام m را به r ارسال می‌کند.

Receive (i,r,m) برای i پیام m را از r دریافت می‌کند.

ب-۱-۲-۲ مشخصات نقش

1- hash function

پروتکل شامل مشخصات نقش برای هر نقش می‌شود. مشخصه نقش، رفتار یک نقش را شرح می‌دهد، که به عنوان دنباله‌ای متناهی از ارسال و دریافت رویدادها نشان داده می‌شود. دانش اولیه نیز به مشخصه نقش تعلق دارد. دانش ابتدایی یک نقش شامل نام‌های دیگر نقش‌ها، کلیدهای عمومی‌تمام نقش‌ها، کلید خصوصی خود آن و غیره می‌شود.

پروتکل کلید عمومیNeedham-Schroeder شامل دو مشخصه، یک مشخصه برای آغازگر و دیگری برای پاسخگو می‌شود.

- برای آغازگر: عاملی که نقش I آغازگر را می‌گیرد، از هویت عاملی که نقش R پاسخگو را می‌گیرد آگاهی دارد و کلید عمومیpk(R) آن در کنار کلید خصوصی sk(I) خود آن قرار می‌گیرد و می‌تواند یک واژه N_i را ایجاد کند.

$$\mathbf{Send}(I, R, \{N_i, I\}_{\mathrm{pk}(R)});$$
$$\mathbf{Receive}(R, I, \{N_i, x\}_{\mathrm{pk}(I)});$$
$$\mathbf{Send}(I, R, \{x\}_{\mathrm{pk}(R)})$$

- برای پاسخگو: عاملی که نقش R پاسخگو را می‌گیرد از هویت عاملی که نقش I آغازگر را می‌گیرد آگاهی دارد و کلید عمومی$\mathrm{pk}(I)$ در کنار کلید خصوصی $\mathrm{sk}(R)$ خود آن قرار می‌گیرد و می‌تواند یک واژه N_i را ایجاد کند.

$$\mathbf{Receive}(I, R, \{y, I\}_{\mathrm{pk}(R)});$$
$$\mathbf{Send}(R, I, \{y, N_r\}_{\mathrm{pk}(I)});$$
$$\mathbf{Receive}(I, R, \{N_r\}_{\mathrm{pk}(R)})$$

ب-۱-۲-۳ رایانش

پیش از آنکه هر رویدادی اجرا شود، هر عامل، رایانش‌هایی را انجام می‌دهد، در حالی که وضعیت پس از هر اجرای رویداد تغییر می‌کند. آنچه که رایانش به طور دقیق انجام می‌دهد، به مدل پروتکل بستگی دارد. در قسمت زیر دو مثال استاندارد از رایانش بیان شده است.

- تطبیق الگو: می‌تواند فرض شود که هر عامل در یک نقش r می‌تواند الگوی هر پیام را ببیند: واژه‌ها، نام‌های عامل، کلیدهای دوره، جفت‌ها، پیام‌های رمزنگاشتی شده و غیره. پیام‌هایی که از تطبیق الگو پیروی نمی‌کنند به طور مستقیم صرف نظر، مجددا ارسال و یا رد خواهد شد.
- استنتاج دانش: مبتنی بر تطبیق الگو، هر عامل شامل مهاجم می‌تواند دانش جدید را از دانش ابتدایی خود همراه با پیام‌های از پیش دریافت شده استنتاج شود. دانش یک عامل از

دانش‌های ابتدایی آن یا پیام‌های دریافت شده با استفاده از قابلیت آن برای تغییر و ویرایش آنها مانند ترکیب، تغییر ترکیب، رمزنگاشتی، رمزگشایی و غیره بدست می‌آید.

ب-۲ انتقال وضعیت

در این مثال، نقش‌ها می‌توانند رویدادها را به صورت همزمان اجرا کنند و هر رویداد می‌تواند چندین بار به صورت نامحدودی تکرار شود.

ب-۲-۱ مدل مهاجم

شبکه می‌تواند تا قسمتی و یا به طور کامل تحت کنترل یک مهاجم باشد. مبتنی بر این دانش، وی می‌تواند برای مثال پیام‌ها را بگیرد، استراق سمع و یا جعل کند. مهاجم می‌تواند پروتکل درحال جریان را نیز قطع یا مختل کند.

دانش ابتدایی K_A^0 یک عامل A در یک نقش برای مثال شامل نام‌ها و کلیدهای عمومی‌تمام عامل‌ها و کلید خصوصی عامل و نقش آن می‌شود. دانش ابتدایی K_1^0 شامل دانش ابتدایی تمام عامل‌های غیرمطمئن از جمله کلیدهای خصوصی آنها می‌شود. دانش یک عامل از جمله مهاجم طی اجرای پروتکل هرزمان که پیام‌ها را دریافت یا می‌گیرد افزایش خواهد یافت.

ب-۲-۲ وضعیت پیکربندی

وضعیت پیکربندی تا حدی طی اجرا پروتکل P مرکب است از دانش مهاجم محلی و دانش محلی هر عامل ممکن A_n، که در آن n در اعداد طبیعی متغیر است. فهرست عامل‌ها نا محدود است به گونه‌ای که این واقعیت را منعکس می‌کند که مهاجم می‌تواند دوره جدیدی را در هر مرحله آغاز کند و دوره‌های نامحدودی را اجرا کند. در وضعیت ابتدایی، هر عامل در وضعیت ابتدایی آن، یعنی دانش ابتدایی و وضعیت کنترل ابتدایی قرار دارد. درصورتی که عامل A_n هنوز فعال نشده باشد، دانش ابتدایی آن تهی است.

قوانین انتقال وضعیت یک پروتکل P چگونگی اینکه وضعیت‌های پیکربندی طی اجرا پروتکل تغییر می‌کنند را شرح می‌دهند. در قسمت زیر ۳ قانونی که نحوهای عملیاتی پروتکل P را تشکیل می‌دهند بیان شده‌اند.

- **نمونه‌های جدید** در صورتی که یک عامل یک رویداد نمونه جدید را اجرا کند، یک نمونه نقش جدید را به وضعیت خود افزوده است. این امر مبتنی بر این فرض است که تعداد نامحدود معرفی نقش امکان پذیر است. عامل زمانی که این نقش را گرفت اجرا می‌کند و سپس دانش ابتدایی به نقش اختصاص می‌یابد. درصورتی که عامل در خطر باشد، تمام دانش را با مهاجم به اشتراک می‌گذارد.
- **رویداد ارسال** درصورتی که عامل یک رویداد ارسال را اجرا کند، پیام ارسال شده m به دانش مهاجم افزوده می‌شود. سپس عامل رایانش‌هایی را اجرا می‌کند و بسته به نتیجه رایانش، به وضعیتی حرکت می‌کند که برای روید ارسال و یا دریافت یا توقف دیگر انتظار می‌کشد.

- **رویداد دریافت** درصورتی که عامل یک رویداد دریافت را اجرا کند، عامل رایانش‌هایی را اجرا می‌کند. بسته به نتیجه رایانش به وضعیتی حرکت می‌کند که برای روید ارسال و یا دریافت یا توقف دیگر انتظار می‌کشد. رایانش‌ها برای مثال شامل آزمایش خوانایی می‌شود. درصورتی که پیام دریافت شده m آزمایش خوانایی را با موفقیت سپری کند، پیام به دانش عامل افزوده خواهد شد.

ب-۲-۳ ردیابی‌ها

انتقال وضعیت نتیجه محدودیت بسیاری از کاربردهای قوانین بالا است که از وضعیت ابتدایی آغاز می‌شود. ردیابی پروتکل P شرح هر انتقال وضعیت ممکن است که از وضعیت ابتدایی آغاز می‌شود:

$$(K_1^0, \langle K_{A_n}^0 \rangle_n) \xrightarrow{m_1} \dots \xrightarrow{m_\ell} \left(K_I^\ell, \langle K_{A_n}^\ell \rangle_n\right) \xrightarrow{m_{\ell+1}} \left(K_I^{\ell+1}, \langle K_{A_n}^{\ell+1} \rangle_n\right) \xrightarrow{m_{\ell+2}} \dots$$

در اینجا ℓ، ℓ مین مرحله انتقال را مشخص می‌کند و m_ℓ پیام تبادل شده در ℓ مین انتقال است. $\langle K_{A_n}^\ell \rangle_n$ و K_I^ℓ به ترتیب دانش محلی عامل A و مهاجم I در ℓ مین مرحله را نشان می‌دهند. $\langle K_{A_n}^\ell \rangle_n$ مخففی برای فهرست نامحدود $K_{A_n}^\ell$ است که در آن n در اعداد طبیعی متغیر است. ارتباط میان m_ℓ و $m_i, i < m,$ به وسیله مشخصه پروتکل تصمیم گیری می‌شود.

ب-۳ ویژگی‌های ردیابی

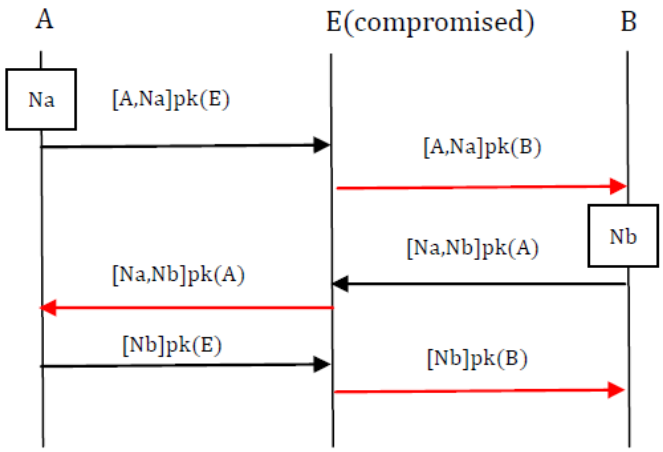
درمیان بسیاری از ویژگی‌های امنیتی در اینجا دو ویژگی ردیابی نشان داده می‌شود: محرمانه بودن و تصدیق.

ب-۳-۱محرمانه بودن

محرمانه بودن بیان می‌کند که اطلاعات معینی نمی‌تواند برای هر عامل دیگر یا مهاجمی‌فاش شود، مگر عامل‌های صادقی که پروتکل را اجرا کرده اند، حتی اگر پروتکل در یک شبکه غیرمطمئن اجرا شود. به طور رسمی‌تر، یک پروتکل P محرمانه بودن پیام m را در میان عامل‌های مطمئن $A_{n1}, \dots, A_{np}$ ایفا می‌کند، اگر و تنها اگر در ردیابی اختیاری، m نتواند از دانش هیچکس دیگری استنتاج شود، یعنی،

$$\mathcal{K}_A^\ell \nvdash m \text{ و } \mathcal{K}_I^\ell \nvdash m$$

برای هر ℓ، که در آن A یکی از $A_{n1}, \dots, A_{np}$ نیست و $\mathcal{K} \vdash m$مشخص می‌کند که m می‌تواند از دانش محلی $\mathcal{K}$ استنتاج شود. در مورد پروتکل کلید عمومیNeedham-Schroeder، مسئله محرمانه بودن این است که اگر $\mathcal{K}_I^\ell \nvdash N_r$ برای گشتاور ℓ در یک ردیابی اگر نقش‌های I و R به وسیله دو عامل مطمئن ایفا شود. حمله انسان درمیانه (man-in-the-middle) که توسط G. Lowe در برابر پروتکل کلید عمومیNeedham-Schroeder مطرح شده است، نشان می‌دهد که محرمانه بودن N_b تولید شده به وسیله یک عامل مطمئن B تضمین شده نیست.



شکل ب-۱- حمله میانی انسان (G.Lowe 1995)

محرمانه بودن به طوری که تعریف شده است می‌تواند به محرمانه بودن ضعیف اشاره داشته باشد، چراکه در آن فاش شدن قسمتی از محتوای پیام اهمیتی ندارد. همچنین محرمانه بودن احتمالی، غیرقابل تشخیص بود و غیره نیز وجود دارد. اما این موارد خارج از محدوده بحث هستند.

ب-۳-۲ تصدیق

هیچ اتفاق نظری درمورد معنای تصدیق وجود ندارد. درواقع سلسله مراتبی از ویژگی‌های تصدیق وجود دارد که به وسیله *Lowe* نشان داده شده است: برقراری، تازگی، توافق (غیر-) نگاشتی، همزمان سازی (غیر-) نگاشتی و غیره. G.Lowe برای مثال توافق غیرنگاشتی را به صورت پیش رو شرح داده است:

آغازگر i در توافق با پاسخگو r است که هرگاه که i به عنوان آغازگر اجرای یک پروتکل را به r تکمیل کند، r به عنوان پاسخگو پروتکل را با i اجرا کرده است. به علاوه، i و r درمورد تمام متغیرهای داده توافق دارند.

توافق نگاشی بیشتر بر این امر تکیه می‌کند که هر اجرای i با یک اجرای انحصاری r مطابقت دارد.

هرچند مشخصه رسمی‌تصدیق می‌تواند از یک ابزار به ابزار دیگر به روشی دقیق بسته به زبان مشخصه و نحوهای عملیاتی متفاوت است. در اینجا درکی شهودی درمورد (عدم-) توافق به عنوان یک ویژگی ردیابی ارائه می‌شود. ابتدا نیاز به معرفی رویداد دیگری با استفاده از یک گزاره دودویی Claim وجود دارد.

Claim (r,NI-Agree) برای توافق غیرنگاشتی برقرار برای نقش r

هر ردیابی یک پروتکل P می‌تواند شامل تعدادی از نمونه‌های رویداد درخواست باشد. به منظور اینکه توافق غیرنگاشتی برای نقش r برقرار می‌شود، مطلب پیش رو باید برقرار باشد:

هر ردیابی که در آن رویداد درخواست در مرحله انتقال ℓ_4 به وسیله یک عامل مطمئن A که تنها با عامل‌های مطمئن ارتباط دارد اجرا می‌شود، هر تبادل پیش بینی شده یک پیام تا نقطه درخواست در پروتکل باید به وسیله عامل‌های مطمئن پیش بینی شده پیش از مرحله انتقال ℓ_4 در ردیابی مشابه اجرا شده باشد.

به بیان غیررسمی‌تر، توافق غیرنگاشتی برای r برقرار می‌شود، زمانی که رویداد درخواست معرفی شده (A, NI-Agree) به وسیله عامل مطمئن A در انتقال ℓم یک ردیابی اجرا شود و زمانی که فرض بر این است که ردیابی تنها به وسیله عامل‌های مطمئن ایجاد شود، سپس تمام پیام‌های تبادل شده میان دو عامل مطمئن A, A'' که فرض شده‌اند که رویدادهای ارسال و دریافت را مطابق با پروتکل پیش از رویداد درخواست اجرا شده‌اند، باید به وسیله A, A'' پیش از مرحله ℓم در ردیابی مشابه ارسال یا دریافت شده باشد.

در مورد پروتکل کلید عمومی Needham-Schroeder

$$\begin{array}{ll} \mathbf{Send}(I,R,\{N_i,I\}_{\mathrm{pk}(R)}); & \mathbf{Receive}(I,R,\{y,I\}_{\mathrm{pk}(R)}); \\ \mathbf{Receive}(R,I,\{N_i,x\}_{\mathrm{pk}(I)}); \quad \text{and} & \mathbf{Send}(R,I,\{y,N_r\}_{\mathrm{pk}(I)}); \\ \mathbf{Send}(I,R,\{x\}_{\mathrm{pk}(R)}) & \mathbf{Receive}(I,R,\{N_r\}_{\mathrm{pk}(R)}) \\ \mathbf{Claim}(I,\mathbf{NI-Agree}) & \mathbf{Claim}(R,\mathbf{NI-Agree}) \end{array}$$

انسان در حمله میانی در شکل ب-۱ بیان می‌کند که توافق غیرنگاشتی برای نقش پاسخگو خراب شده است: عامل مطمئن B معتقد است که با عامل مطمئن A ارتباط برقرار کرده است و فرض براین است که پیام $\{N_b\}_{pk(B)}$ به وسیله عامل مطمئن A ارسال شده اما از سوی عامل درخطر E جعل شده باشد.

پیوست پ

(اطلاعاتی)
مثال‌های تصدیق

پ-۱ پروتکل نمونه

این پیوست نمونه‌ها و محصولات طراحی تصدیق پروتکل را ارائه می‌دهد.

$$S_1)\ A \rightarrow B: \{N_A, A\}_{K\,(B)}$$
$$S_2) B \rightarrow A: \{N_A, N_B, B\}_{K\,(A)}$$
$$S_3)\ A \rightarrow B: \{N_B\}_{K(B)}$$

شکل پ-۱ پروتکل تصدیق کلید عمومی Needham-Schroeder

این پروتکل قسمت تصدیق به خوبی مطالعه شده پروتکل کلید عمومی Needham-Schroeder است که توسط Lowe تصحیح شده است. از این پس به این پروتکل به عنوان پروتکل NSL اشاره می‌شود.

شکل پ-۱ این پروتکل را به صورت نمادگذاری غیررسمی "Alice-and-Bob" نشان داده است. این پروتکل شامل سه مرحله S_1 تا S_3 می‌شود که در آنها A و B به منظور تصدیق متقابل یک دیگر پیام‌هایی را مبادله می‌کنند. N_A و N_B واژه‌ها را نمایش می‌دهد و نماد $\|$ جهت چندتایی کردن مورد استفاده قرار می‌گیرد و زیروندهای $K\,(A)$ و $K(B)$ رمزنگاشتی کلیدعمومی‌را با کلیدهای عمومی‌عامل‌های A و B نشان می‌دهد. بنابراین، در این پروتکل فرض براین است که کلیدها از پیش توزیع شده‌اند؛ پروتکل اصلی Needham-Schroeder برای این منظور از یک خدمت رسان اصلی استفاده کرده است.

الزامات غیررسمی‌برای این پروتکل می‌تواند به صورت زیر خلاصه شود:

محرمانه بودن واژه برای N_A: در یک پروتکل میان عامل‌های مطمئن، A و B، واژه N_A تبادل شده تنها برای آنها شناخته شده است (و به طور خاص، برای متجاوز شناخته شده نیست).

محرمانه بودن واژه برای N_B: که به صورت متشابه بیان می‌شود.

تصدیق B: درصورتی که A نقش خود را با عاملی که گمان می‌کند که B باشد تکمیل کند، B نیز پروتکل را اجرا می‌کند.

تصدیق A: به صورت متشابه تنظیم می‌شود.

پ-۲ محصولات طراحی

در اینجا چگونگی اینکه این پروتکل می‌تواند با توجه به چهار هدف تصدیق شود شرح داده شده است. این نمونه‌ای برای PAL2 (تصدیق محدود) و OFMC[1] است، مدل شبکه‌ای در حال جنبش به عنوان ابزار تصدیق مورد استفاده قرار می‌گیرد. به ویژه، به عنوان قسمتی از ابزار AVISPA مورد استفاده قرار می‌گیرد. این ابزار می‌تواند به طور مستقیم در وب مورد استفاده قرار گیرد و نسخه وب همراه با کتابخانه‌ای ارائه می‌شود که شامل مثال NSL می‌شود که در اینجا نشان داده شده است.

1- the On-the-Fly Model Checker

پ-۲-۱ ورودی ابزار تصدیق پروتکل

پروتکل NSL قسمتی از کتابخانه AVISPA است که همراه با توزیع AVISPA ارائه می‌شود. در این کتابخانه، "NSPK-fix" نامیده می‌شود و یکی از مثال‌های مشابه است. از آنجایی که این موردی برای تمام پروتکل‌ها در کتابخانه AVISPA است، این پروتکل به زبان سطح بالای HLPSL مشخص می‌شود

```
role alice (A, B: agent,Ka, Kb: public_key, SND, RCV: channel (dy))
 played_by A def=
 local State : nat, Na, Nb: text
 init State := 0
 transition
 0. State = 0 /\ RCV(start) =|> State':= 2 /\ Na' := new() /\ SND({Na'.A}_Kb)
 /\ secret(Na',na,{A,B}) /\ witness(A,B,bob_alice_na,Na')
 2. State = 2 /\ RCV({Na.Nb'.B}_Ka) =|> State':= 4 /\ SND({Nb'}_Kb) /\
 request(A,B,alice_bob_nb,Nb')
 end role
 role bob(A, B: agent, Ka, Kb: public_key, SND, RCV: channel (dy))
 played_by B def=
 local State : nat, Na, Nb: text
 init State := 1
 transition
 1. State = 1 /\ RCV({Na'.A}_Kb) =|> State':= 3 /\ Nb' := new() /\ SND({Na'.Nb'.B}_Ka)
 /\ secret(Nb',nb,{A,B}) /\ witness(B,A,alice_bob_nb,Nb')
 3. State = 3 /\ RCV({Nb}_Kb) =|> State':= 5 /\ request(B,A,bob_alice_na,Na) end role
 role session(A, B: agent, Ka, Kb: public_key) def=
 local SA, RA, SB, RB: channel (dy)
 composition alice(A,B,Ka,Kb,SA,RA) /\ bob (A,B,Ka,Kb,SB,RB)
 end role
 role environment() def=
 const a, b : agent,
 ka, kb, ki : public_key,
 na, nb, alice_bob_nb, bob_alice_na : protocol_id
intruder_knowledge = {a, b, ka, kb, ki, inv(ki)}
 composition session(a,b,ka,kb) /\ session(a,i,ka,ki) /\ session(i,b,ki,kb)
 end role
 goal
 secrecy_of na, nb
 authentication_on alice_bob_nb
authentication_on bob_alice_na
 end goal
environment()
```

شکل پ- ۳رسمی‌سازی HLPSL پروتکل NSL

HLPSL زبانی است که برای مشخص کردن فعالیت‌های عامل‌ها (که در نقش‌های مختلف پروتکل عمل می‌کنند) به عنوان سامانه‌های انتقال به خوبی منطبق شده است. این زبان مبتنی بر فعالیت‌های منطق موقتی Lamport، زبانی که خود نحوهای انتقال وضعیت را دارد، می‌باشد همانطور که می‌تواند در شکل پ-۲ نشان داده

شده است، یک فایل HLPSL ورودی‌های مورد نیاز را فراهم می‌آورد. جزئیات بیشتر در قسمت زیر نشان داده شده است.

پ-۲-۲ مشخصه پروتکل

پروتکل خود با اظهار نقش‌ها برای عامل‌های مختلف (در اینجا "alice" و "bob" و در رسمی‌سازی دیگر «آغازگر» یا «پاسخگو» نامیده می‌شود). این موارد به طور ضروری، به عنوان ماشین‌های وضعیت توسعه یافته، که سامانه‌های انتقالی هستند که متغیر وضعیت محلی می‌تواند در زمان انتقال به روز رسانی شود، رسمی‌شده‌اند. پیرو قرارداد TLA، متغیرهای نخستین به مقادیری در وضعیت‌های جانشین اشاره دارد. بنابراین، برای مثال، *وضعیت* (State) نقطه کنترل پیش از انتقال و وضعیت نقطه کنترل پس از انتقال را نشان می‌دهد. انتقال‌ها خود به صورت فرمول‌هایی رسمی‌می‌شوند که آنچه را که باید پیش از به طور مستقیم پس از انتقال برقرار باشند را بیان می‌کنند. برای مثال در نقش alice،

0. State = 0 /\ RCV(start) =|> State':= 2 /\ Na' := new() /\ SND({Na'.A}_Kb)
/\ secret(Na',na,{A,B}) /\ witness(A,B,bob_alice_na,Na')

به صورت رسمی‌بیان می‌کند که اگر عامل در نقش خود در وضعیت شروع خود (۰) قرار داشته باشد و پیام شروع را دریافت کند، می‌تواند انتقال به وضعیت جانشین (۲) را بگیرد، یک واژه ’Na جدید را تولید کند و یک پیام مناسب را ارسال کند. اصطلاحات محرمانه و شاهد در خط دوم اطلاعات افزوده دفترداری هستند تا فرمول سازی ویژگی‌های امنیتی را تسهیل کند (متشابه با رویدادهای علامت دهی مانند اجرا (running) و متعهد شدن (commit). آنها ضرورتا ثبت می‌کنند که واژه ’Na تولید شده باید اشتراک محرمانه میان A و B باشند و اینکه عامل A (قبول شده به عنوان یک پارامتر نقش) پروتکل را شروع کرده است، برای ارتباط داشتن با عامل B درنظر گرفته شده است و اینکه آنها باید درمورد مقدار موارد داده‌ای معین موافق باشند. این مثال برای نقش alice و bob با PPS_MECHANIZED مطابقت دارد.

در مرحله بعد، علامتگذاری یک دوره پروتکل تعریف می‌شود. یعنی ترکیب (نشان داده شده به وسیله ترکیب عطفی) عامل‌هایی که در نقش Alice و Bob عمل می‌کنند.

پ-۲-۳محیط عملیاتی

در اصل، باید ذکر شود که هر عامل در یک مجرای *dy* ارتباط برقرار می‌کند. این امر "Dolev-Yao" را نشان می‌دهد و اظهار می‌کند که متجاوز به تمام پیام‌های تبادل شده دسترسی داشته است و به عنوان یک متجاوز استاندارد Dolev-Yao رفتار کرده است. در قسمت *محیط* مشخصه، یک طراح پروتکل به طور مقادیر ثابت گوناگون و همچنین آنچه را که متجاوز از ابتدا می‌داند را اظهار می‌کند. همانطور که در اینجا مشخص شده است، وی نام تمام عامل‌ها (a و b)، کلیدهای عمومیو جفت کلید خصوصی/عمومی‌خود را می‌داند. به علاوه، طراح پروتکل شماره و نوع دوره‌هایی را که می‌توانند به صورت همزمان اجرا شوند را مشخص می‌کند. این مسئله سه دوره را مشخص می‌کند: یک دوره میان عامل‌های مطمئن (با نام a و b) و دو در جایی که متجاوز (عامل با نام i) می‌تواند یا آغازگر باشد و یا پاسخگو. این شرح با POE_FORMAL مطابقت دارد.

پ-۲-۴ویژگی‌های امنیتی

بیان‌های هدف، چهار هدف را که به صورت غیر رسمی در قسمت‌های قبل عنوان شده‌اند را رسمی می‌کند: محرمانه بودن واژه (برای هر دو واژه) و تصدیق (برای هر دو عامل). تمام چهار مورد پشت خط ابزار AVISPA به عنوان ورودی یک زبان سطح پایین تر که IF نامیده می‌شود ، برای **قالب متوسط**، در نظر گرفته می‌شود. ابزار AVISPA به صورت خودکار فایل‌های HLPSL را به فایل‌های IF پیش از اجرای پشت خط تبدیل می‌کند. مستند سازی برای IF می‌تواند در صفحه خانگی AVISPA یافت شود. IF یک زبان طبقه بندی شده است که انتقال‌ها به عنوان قواعد بازنویسی چندمجموعه‌ای (“.“ اشتراک چندمجموعه است) بیان می‌شوند. یعنی، وضعیت سامانه یک چندمجموعه‌ای هسته‌ها است که وضعیت‌های عامل‌های مختلف و دانش متجاوز را شرح می‌دهد. انتقال‌ها چگونگی اینکه این وضعیت به روزرسانی می‌شود را شرح می‌دهد. باید توجه شود که شبکه به طور مستقیم با متجاوز شناسایی می‌شود بنابر این بیش از ارسال و دریافت پیام‌ها، تاثیر یک عاملی که یک مرحله پروتکل را می‌پذیرد، به روزرسانی دانش متجاوز (رسمی‌شدن با استفاده از iknows) است. ویژگی‌های امنیتی در IF به عنوان گزاره‌هایی در وضعیت‌هایی که وضعیت‌های غیرایمن (برای مثال attack_state secrecy_of_na) را توصیف می‌کنند، رسمی‌می‌شوند. یک مورد از چنین گزاره‌هایی برای هر یک از چهار هدف امنیتی وجود دارد. این شرح با PSP_FORAML مطابقت دارد.

پ-۲-۵ گواه

در اینجا، گواه تصدیق پروتکل ارائه شده به وسیله ابزار تصدیق نشان داده شده است.

```
OFMC
SUMMARY
SAFE
DETAILS
BOUNDED_NUMBER_OF_SESSIONS

PROTOCOL
/home/avispa/web-interface-computation/./tempdir/workfileA26980.if
GOAL
as_specified

BACKED
OFMC

COMMENTS

STATISTICS
parseTime:0.00s
searchTime:0.17s
visitedNodes:105 nodes
depth:8 plies
```

شکل پ-۳ خروجی AVISPA/OFMC

شکل پ-۳ خروجی ابزار AVISPA را که OFMC را در مشخصه IF از NSPK اجرا می‌کند را نمایش می‌دهد. این خروجی یک تصدیق محدود است: بررسی تمام روش‌هایی که سه دوره مشخص شده می‌توانند جای گذاری شوند. برای پروتکل‌هایی در این اندازه و تنها با سه دوره، OFMC بسیار سریع است. OFMC درختی با عمق ۸ که ۱۰۵ گره را بررسی می‌کند، جستجو می‌کند. در اینجا باید تاکید شود که اگرچه اندازه نسبتا کوچک این فضای جستجو به دلیل استفاده از تکنیک‌های نمایش نمادین مبتنی بر یک حساب محدود شده تخصصی و هم استفاده از تفکیک محدود شده کاهش تعداد جای گذاری‌های ممکن است.

باید یادآور شد که ابزار AVISPA تنها برای یک مورد اجازه مشخص کردن نمونه‌های دوره **عینی (Concrete)** را در قسمت محیط مشخصه HLPSL فراهم می‌کند. این یک محدودیت ناخوشایند است. درصورتی که یک طراح پروتکل به تصدیق محدود برای نمونه‌های دوره n (موازی) تمایل داشته باشد، مجبور است به طور محدود بسیاری از سناریوهای مختلف را در مورد عامل‌های مختلف که نقش‌های مختلفی را ایفا می‌کنند به صورت دستی تولید کند. درحالی که انجام این کار به صورت خودکار ساده است، تولید و بررسی تمام چنین نمونه‌هایی به طور اساسی زمان تصدیق را افزایش می‌دهد.

یادآوری- درصورتی که نقش‌های n موجود باشند و کران بالا $(n+1)^n$ باشد، هریک از عامل‌های مطمئن n یا مهاجم می‌تواند در هر نقشی عمل کند. به صورت کلی، سناریوهای کمی‌وجود دارند که مهاجم مجاز به ایفای برخی از نقش‌ها نخواهد بود (برای مثال، به عنوان خدمت رسان کلیدی مورد اطمینان) و سناریوها تنها شامل جایگشت‌های نام‌های عامل‌های مطمئن می‌توانند متناظر درنظر گرفته شوند.

خوشبختانه OFMC از روشی جهت مشخص کردن حدهای دوره به صورت مستقیم پشتیبانی می‌کند. اگرچه، این مسئله هنوز به وسیله ابزار AVISPA پشتیبانی نمی‌شود، مانند مشخصه باید به طور مستقیم در IF صورت گیرد.

به عنوان مثال این مورد، یک طراح پروتکل می‌تواند کد IF تولید شده از مشخصه HLPSL را به وسیله ابزار AVISPA بپذیرد و به صورت دستی دوره‌های پایه را با مشخصه‌های نمادین جایگزین کند. در این مثال، طراح پروتکل باید چهار خط زیر را که دوره‌های نخستین (پایه) را اظهار می‌کند.

```
state_alice(a,b,ka,kb,0,dummy_nonce,dummy_nonce,set_62,3).
state_bob(b,a,ka,kb,1,dummy_nonce,dummy_nonce,set_70,4).
state_alice(a,i,ka,ki,0,dummy_nonce,dummy_nonce,set_74,6).
state_bob(b,i,ki,kb,1,dummy_nonce,dummy_nonce,set_78,10)
```

با بیان نمادین دوره زیر جایگزین کند:

```
state_alice(A1,B1,Ka1,Kb1,0,dummy_nonce,dummy_nonce,set_62,3).
state_bob(B2,A2,Ka2,Kb2,1,dummy_nonce,dummy_nonce,set_70,4).
state_alice(A3,B3,Ka3,Kb3,0,dummy_nonce,dummy_nonce,set_74,6).
state_bob(B4,A4,Ka4,Kb4,1,dummy_nonce,dummy_nonce,set_78,10)
```

در اینجا مقادیر ثابت به آسانی جایگزین می‌شوند. بیان جدید نشان می‌دهد که دو عامل قصد دارند در نقش Alice، آغازگر ایفای نقش کنند و دو عامل قصد دارند نقش Bob، پاسخگو را بازی کنند. هنگام جستجوی

حملات با استفاده از حل محدودیت‌ها، OFMC تمام نمونه‌های مرتبط این متغیرها را با نام‌های عامل‌های ممکن شامل متجاوز تولید خواهد کرد.

SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
nspk-fix-sumb.if

GOAL
as_specified

BACKEND
OFMC

COMMENTS

STATISTICS
parseTime:0.00s
searchTime:0.20s
visitedNodes:102 nodes
depth:8 plies

شکل پ-۴ خروجی OFMC با دوره‌های نمادین

با تعین این مشخصه نمادین، OFMC مانند شکل پ-۴ پاسخ می‌دهد، بنابراین پروتکل را در مورد دو دوره موازی تصدیق می‌کند. به طور قابل توجه، با استفاده از نام‌های نشانه این فضای جستجو کمی‌در این مثال کوچکتر است. این گواه با PEV_BOUNDED مطابقت دارد.

پ-۳ ورودی‌های افزوده برای تصدیق

ورودی‌های ویژه ابزار جهت تصدیق در قسمت بالا مستند شده‌اند. ورودی‌های افزوده برای تصدیق پروتکل در این قسمت شرح داده می‌شوند. اول این‌که، توسعه دهنده باید نشان دهد که خود ابزار مبتنی بر یک مبنای نحوی صدا است. این مورد برای OFMC صدق می‌کند. Basin و همکاران یک حساب با دقت تعریف شده را برای تصدیق پروتکل‌های مشخص شده به یک زبان ورودی را که اساسا IF است ارائه می‌دهند. حساب، درکنار بهینه سازی‌های گوناگون (مطابق با مواردی که به وسیله OFMC مورد استفاده قرار می‌گیرد) درست و کامل نشان داده شده‌اند. مطمئنا این موارد دلایل دستی هستند، اما دستخوش بررسی دقیق قابل توجهی قرار گرفته اند که در یک مجله درجه یک منتشر شده‌اند.

دوم این که، توسعه دهنده باید گواه‌هایی را ارائه دهد که ابزار به درستی به‌کارگرفته شده است. OFMC به زبان Haskell که یک زبان برنامه نویسی اعلانی است، نوشته شده است. این زبان باید بررسی یک کد را درجایی که مستند سازی روابط میان ابزار و حساب امکان پذیر باشد را ساده کند. این امر هنوز رخ نداده است.

یادآوری ۱- گواه موجود برای صحت OFMC از آزمون گسترده بر روی کتابخانه AVISPA و این واقعیت که نتایج با موارد شناخته شده از مکتوبات مطابقت دارد بدست می‌آید.

باید یادآور شد که اگر AVISPA به عنوان نتیجه نهایی برای OFMC مورد استفاده قرار می‌گیرد، التزام‌های افزوده‌ای در اینجا برای نشان دادن اینکه نگاشت از HLPSL به IF حفظ معانی است وجود دارد. گزینه دیگر در اینجا مشخص کردن پروتکل به طور مستقیم در IF است.

سوم، گواهی کننده باید تضمین کند که ویژگی‌ها به درستی مشخص شده‌اند و توسعه دهنده باید مستند سازی را جهت کمک به این وظیفه ارائه دهد. در مورد OFMC این امر درست است: اگرچه کلمات کلیدی ویژه برای مشخص کردن ویژگی‌ها در HLPSL وجود دارد، تبلور نحوی ساده برای گزاره‌های مشخص شده در IF وجود دارد. این گزاره‌ها دارای نحوهای به خوبی تعریف شده‌ای هستند (این نحوها به روشی آسان در وضعیت‌های سامانه انتقال طی بررسی مدل تفسیر می‌شوند).

یادآوری ۲- توافق غیر نگاشتی برای یک متجاور A با یک پاسخگوی B در مجموعه‌ای از اقلام داده‌ای ds بیان می‌کند که هرگاه A (عامل به عنوان متجاوز) اجرای پروتکل را به اتمام برساند، ظاهرا با پاسخگوی B، سپس B از پیش پروتکل را اجرا کرده باشد، ظاهرا با A و B به عنوان یک پاسخگو در اجرای خود عمل کرده باشد و دو عامل درمورد مقادیر داده مطابق با تمام متغیرها در ds توافق داشته باشند. این مورد غیر نگاشتی است، چراکه رابطه یک-یک میان اجرای A و اجرای B را ضمانت نمی‌کند.

در نهایت، توسعه دهنده باید به روشنی روشی که مدل را محدود کرده است و به‌کارگیری آن را بیان کند. در نسخه حال حاضر HLPSL، محدوده‌های دوره با فهرستی از نمونه‌های دوره عینی تعیین شده‌اند. بنابراین پروتکل با توجه به تمام جاگذاری ممکن عامل‌های اجرا کننده این دوره‌ها و همچنین جاگذاری‌ها با پیام‌های ممکن ارسال شده به وسیله متجاوز تصدیق می‌شود. زمانی که OFMC به طور مستقیم، بدون AVISPA نهایی مورد استفاده قرار گیرد، مشخص کردن دروه‌های نمادین ممکن است، که اظهار مستقیم تعداد ثابت دوره‌ها را بدون تعهد نسبت به نام‌های عامل‌های ایفا کننده در هر نقش امکان پذیر می‌کند.