INSO

21834
1st.Edition

2017

Identical with
ISO-IEC-IEEE-
18883
(2016)

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران

Iranian National Standards Organization

استاندارد ملی ایران
۲۱۸۳۴

چاپ اول

۱۳۹۶

دارای محتوای رنگی

فناوری اطلاعات – شبکه واپایش (کنترل) انجمن سبز همه جا حاضر – امنیت

Information technology — Ubiquitous green community control network — Security

ICS: 35.110

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج ، شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.gov.ir

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri .gov.ir

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

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

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و کسب‌وکار است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی‌و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های 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 می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و الزامات خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، پیاده‌سازی بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، پیاده‌سازی استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سامانه‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها 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 for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد
«فناوری اطلاعات - شبکه واپایش (کنترل) انجمن سبز همه جا حاضر - امنیت»

رئیس:	سمت و/ یا محل اشتغال:
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا دانشگاه تربیت مدرس
دبیر:	
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات، گرایش تکنولوژی ارتباطات)	مشاور مرکز آپا دانشگاه تربیت مدرس
اعضا: (اسامی به ترتیب حروف الفبا)	
اسدی پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
ترابی، مهرنوش (فوق لیسانس مهندسی فناوری اطلاعات- تجارت الکترونیک)	کارشناس استاندارد
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
صالحی، فاطمه (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس مسئول پرداخت الکترونیک شرکت فناوری اطلاعات و ارتباطات بانک پاسارگاد (فناپ)
قندهاری، آزاده (فوق لیسانس کامپیوتر، نرم‌افزار)	عضو هیات علمی دانشگاه آزاد اسلامی واحد ساوه و کارشناس مرکز تحقیقات مخابرات ایران
کماسی، مهدی (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس شرکت گسترش سرمایه‌گذاری ایران خودرو
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر دانشگاه تربیت مدرس

معروف، سینا — کارشناس سازمان فناوری اطلاعات ایران

(لیسانس، مهندسی کامپیوتر، سخت افزار)

ویراستار:

فرهاد شیخ احمد، لیلا — کارشناس استاندارد

(فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات - شبکه واپایش انجمن سبز همه جا حاضر - امنیت» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی ایران شمارهٔ ۵ تهیه و تدوین شده، در پانصد و هفتمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۹۶/۲/۱۹ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم وخدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC/IEEE 18883:2016, Information technology — Ubiquitous green community control network — Security

مقدمه

این استاندارد کارکرد مدیریت امنیت بهبودیافته برای پروتکل تعریف‌شده در استاندارد™ IEEE1888[1] را توصیف می‌کند، استاندارد IEEE برای پروتکل شبکه واپایش انجمن سبز همه جا حاضر، الزامات امنیتی را مشخص می‌کند، معماری امنیتی سامانه را تعریف می‌کند، توصیفی استاندارد از اصالت‌سنجی و مجوزدهی را همراه با روش‌های امنیتی و پروتکل‌ها ارائه می‌دهد. این استاندارد می‌تواند به جلوگیری از افشای ناخواسته داده‌ها در مقابل دسترسی عمومی و غیر مجاز منابع کمک می‌کند، در حالی که یکپارچگی و محرمانگی بهبودیافته داده‌های منتقل شده در شبکه واپایش انجمن سبز همه جا حاضر را ارائه می‌دهد.

هدف از این استاندارد، تعیین و تعریف کارکرد مدیریت امنیت در شبکه واپایش انجمن سبز همه جا حاضر است که بن‌سازه[2] عملیات برنامه‌های کاربردی سازگار با کیفیت بالا و امن را فراهم می‌کند. به عنوان یک سامانه باز، شبکه واپایش انجمن سبز همه جا حاضر، عملیات چند دامنه و دسترسی عمومی سایر مولفه‌های سامانه را فرض می‌کند. در این زمینه، ملاحظات امنیتی برای عملیات پروتکل IEEE 1888 مورد نیاز است.

این استاندارد ویژگی، معماری و چارچوبی که امنیت را برای سامانه‌های IEEE 1888 ارائه می‌کند، تعریف می‌کند. به دلیل پایش تعاملی و سامانه واپایش مبتنی بر شبکه‌های حسگر محرک، سامانه‌های IEEE 1888 بدون امنیت در معرض تهدیدات امنیتی بالقوه است. به عنوان مثال، کاربران یا سامانه‌های ناخواسته ممکن است قرائت حسگر را اخذ کنند و تهویه مطبوع یا چراغ را به راحتی واپایش کنند یا اطلاعات تبادل‌شده و داده‌های ذخیره شده ممکن است توسط کاربران یا مولفه‌های غیر مجاز رونویسی شود. این استاندارد چارچوب امنیتی برای محافظت از مسیر تبادل پیام از سمت داده و سمت واپایش سامانه IEEE 1888 از چنین تهدیدات امنیتی را مشخص می‌کند و اصالت‌سنجی دوجانبه، واپایش دسترسی، یکپارچگی پیام، محرمانگی داده و غیره را ارائه می‌کند.

پروتکل IEEE 1888 به پروتکل دسترسی شی ساده (SOAP)[3] محدود می‌شود و به طور معمول پروتکل انتقال فرامتن (HTTP)[4] برای انتقال پیام‌های SOAP را دربرمی‌گیرد. برای برآورده کردن الزامات امنیتی و محافظت از تهدیدات امنیتی، HTTP در TLS (HTTPS) باید اتخاذ شود. دلیل این موضوع این است که HTTPS به طور گسترده‌ای استفاده می‌شود و می‌تواند الزامات امنیتی با هزینه پیاده‌سازی کوچک را برآورده سازد.

این استاندارد، موضوعات قابلیت اطمینان سامانه را از موضوعات امنیتی متمایز می‌کند. به عنوان مثال، تحمل خدمت در برابر خواست‌های سنگین کارخواهان و تحمل ارتباط در برابر شکست پیوند فیزیکی خارج از دامنه کاربرد این استاندارد است.

1 - Institute of Electrical and Electronics Engineers
2 - Platform
3 - Simple object access protocol
4 - Hypertext transfer protocol

این استاندارد به شرح زیر سازمان یافته است:

- بند ۴ الزامات امنیتی و اصول طراحی را مشخص می‌کند.
- بند ۵ معماری سامانه امنیتی را توصیف می‌کند.
- بند ۶ پروتکل‌های امنیتی، شامل دنباله ارتباطی، واسط نرم‌افزار و سامانه شناسانه (ID)[1] را تعریف می‌کند.

1 - Identifier

فناوری اطلاعات - شبکه واپایش (کنترل) انجمن سبز همه جا حاضر - امنیت

۱ کلیات

۱-۱ دامنه کاربرد

این استاندارد ویژگی پیشرفت‌های خدمت امنیتی برای پروتکل تعریف‌شده در استاندارد IEEE std 1888 برای پروتکل واپایش شبکه انجمن سبز همه جا حاضر را ارائه می‌کند. این استاندارد الزامات امنیتی برای شبکه واپایش انجمن سبز همه جا حاضر را توصیف می‌کند و معماری امنیتی سامانه را همراه با روش‌های اجرایی و پروتکل‌های امنیتی مشخص می‌کند.

۱-۲ هدف

هدف از تدوین این استاندارد، تعریف یک کارکرد مدیریت امنیت در شبکه واپایش انجمن سبز همه جا حاضر است که بن‌سازه عملیات برنامه‌های کاربردی سازگار، با کیفیت بالا و امن را ارائه می‌کند. استفاده از این استاندارد به جلوگیری از افشای ناخواسته داده‌ها به دسترسی عمومی و غیر مجاز به منابع کمک می‌کند، همچنین یکپارچگی و محرمانگی بهبودیافته داده‌های منتقل شده در شبکه واپایش انجمن سبز همه جا حاضر را ارائه می‌کند.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی‌است:

۲-۱ مراجع الزامی

2-1 IEEE Std 1888™, IEEE Standard for Ubiquitous Green Community Control Network Protocol.2,

2-2 RFC 791, Internet Protocol, J. Postel, Ed., September 1981.

2-3 RFC 1035, Domain Names—Implementation and Specification, P. Mockapetris, November 1987.

2-4 RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, R. Housley, W. Ford, W.Polk, and D. Solo, January 1999.

2-5 RFC 2460, Internet Protocol, Version 6 (IPv6) Specification, S. Deering and R. Hinden, December 1998.

2-6 RFC 5246, The Transport Layer Security (TLS) Protocol, Version 1.2, T. Dierks and E. Rescorla, August2008.

2-7 RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)

2-8 Profile, D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, May 2008.

2-9 RFC 5322, Internet Message Format, P. Resnick, Ed., October 2008.

2-10 RFC 6066, Transport Layer Security (TLS) Extensions: Extension Definitions, D. Eastlake, III, January2011.

۲-۲ مراجع بیشتر

2-11 RFC 6277, "Online Certificate Status Protocol Algorithm Agility," S. Santesson and P. Hallam-Baker, June 2011.The OpenSSL Project website.

۳ تعاریف، کوته‌نوشت‌ها و سرنام‌ها

۳-۱ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات و تعاریف زیر به کار می‌رود. استانداردهای فرهنگ لغت برخط IEEE باید برای اصطلاحاتی که در این بند تعریف نشده به کار گرفته شود.[1]

واپایش دسترسی

access control

پیشگیری از استفاده غیر مجاز یک منبع، از جمله پیشگیری از استفاده از منابع به شیوه‌ای غیر مجاز.

اطلاعات انقیاد

binding information

ارتباط شناسانه (ID) گواهی با نقش کارخواه پاسخگو با شناسانه منبع یکنواخت دسترسی (URI)[2] برای پاسخگو همراه با عمر باقی مانده آن انجمن.

محرمانگی

1 - IEEE Standards Dictionary Online subscription is available at: http://www.ieee.org/portal/innovate/products/standard/standards_dictionary.html.
2 - Uniform resource identifier

confidentiality

خصوصیتی که اطلاعات برای افراد، هستارها[1] یا فرآیندهای غیر مجاز در دسترس نباشد یا افشا نشود.

یکپارچگی داده‌ها

data integrity

خصوصیتی که داده‌ها به شیوه‌ای غیر مجاز بدون تشخیص یا آگاهی دچار تغییر یا تخریب نشود.

امضای دیجیتال

digital signature

داده‌های اضافه شده یا تغییر رمزنگاری یک واحد داده که به دریافت‌کننده واحد داده اجازه می‌دهد تا منبع و یکپارچگی واحد داده را درستی‌سنجی و در برابر جعل اسناد محافظت کند.

۲-۳ کوته‌نوشت‌ها و سرنام‌ها

AAA	authentication, authorization, and accounting	اصالت‌سنجی، مجوزدهی و پاسخگویی
ACL	access control list	فهرست واپایش دسترسی
ACM	access control manager	مدیر واپایش دسترسی
AM	authentication manager	مدیر اصالت‌سنجی
APP	application	برنامه کاربردی
CA	certificate authority	مرکز صدور گواهی
CV	certificate verification	درستی‌سنجی گواهی
DNS	domain-name system	سامانه نام دامنه
DoS	denial of service	انکار خدمت
DDoS	distributed denial of service	انکار خدمت توزیع شده
FQDN	fully qualified domain name	نام دامنه کاملا واجد شرایط
GW	gateway	دروازه
HTTP	hypertext transfer protocol	پروتکل انتقال ابرمتن

1 - Entities

HTTPS	hypertext transfer protocol (HTTP) over transport layer security (TLS)	پروتکل انتقال ابرمتن (HTTP) در امنیت لایه انتقال (TLS)
ID	identifier	شناسانه
IP	Internet protocol	پروتکل اینترنت
IPv4	Internet Protocol Version 4	نسخه ۴ پروتکل اینترنت
IPv6	Internet Protocol Version 6	نسخه ۶ پروتکل اینترنت
IV	identifier (ID) verification	درستی‌سنجی شناسانه (ID)
Mal-APP	malicious application (APP)	نرم‌افزار کاربردی مخرب (APP)
OCSP	online certificate status protocol	پروتکل وضعیت گواهی برخط
SAN	subject alternative name	نام جایگزین موضوع
SOAP	simple object access protocol	پروتکل دسترسی شی ساده
TCM	transport layer security (TLS) manager	مدیر امنیت لایه انتقال (TLS)
TLS	transport layer security	امنیت لایه انتقال
TTL	time to live	مدت زمان عمر
UI	user interface	واسط کاربری
URI	uniform resource identifier	شناسانه منبع یکنواخت

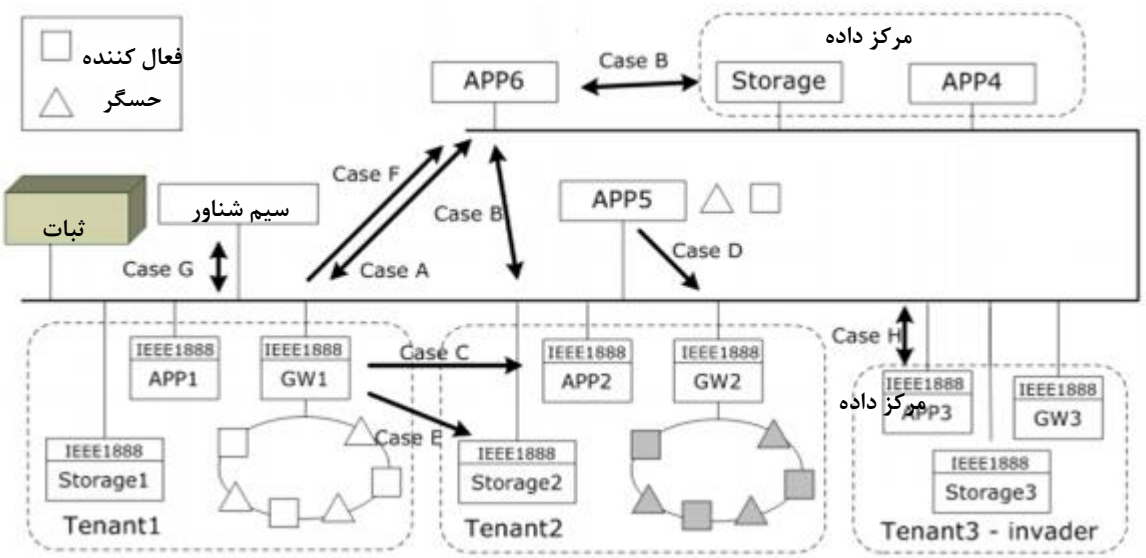
۴ الزامات امنیتی و اصول طراحی

۴-۱ مرورکلی کلی مسائل امنیتی

در یک سامانه نمونه IEEE 1888 (شکل ۱)، دروازه‌های (GWs[1]) اتصال‌دهنده حسگرها و محرک‌ها به صورت توزیع‌شده در مستاجران متعددی مستقر هستند. دروازه‌ها، داده‌ها را از حسگرها به ذخیره‌ساز محلی و ذخیره‌ساز از دور در مرکز داده بارگذاری می‌کنند. مولفه‌های برنامه کاربردی (APP) در مستاجران می‌توانند به صورت جداگانه داده‌ها را از ذخیره‌ساز محلی / از دور بازیابی کند و از آنها برای مقاصد خود (تحلیل داده‌ها یا تجسم داده‌ها و غیره) استفاده کند. مولفه‌های APP همچنین دستورات را به GW ها برای واپایش دیسک ارائه می‌کنند. همانطور که در شکل ۱ نشان داده شده است، APP1 وStorage1 می‌توانند حسگرها /

1 - Gateways

دیسک‌های متصل به GW1 را اداره کند. App2 و Storage2 می‌تواند حسگرها / دیسک‌های متصل به GW2 را اداره کند. APP5 از دور می‌تواند به Tenant1 با مجوز اداره حسگرها / دیسک‌های متصل به GW1 دسترسی پیدا کند.



شکل ۱ - تهدیدات امنیتی بالقوه در سامانه IEEE 1888

همانطور که در شکل ۱ نشان داده شده، تهدیدات امنیتی بالقوه در سامانه IEEE 1888 را می‌توان از **Case A** تا **Case H** بیان کرد.

Case A- یک برنامه کاربردی مخرب (MAL-APP) ممکن است عمدا داده‌ها را از GW ها (واکشی) واکشی کند یا فرمان‌های واپایش را به GW ها (نوشتن) ارسال کند.

Case B– MAL-APP ممکن است عمدا داده‌ها را از ذخیره‌ساز از دور/ محلی (واکشی) واکشی کند یا داده‌ها را روی ذخیره‌ساز (نوشتن) بازنویسی کند.

Case C– APP ممکن است ناخواسته داده‌هایی را که از GW ها یا ذخیره‌ساز (واکشی) به کاربران خود محدود نیست، بگیرد. به عنوان مثال، App2 ممکن است داده‌ها را از GW1 که در مستاجر یکسان نیست به دست آورد.

Case D-APP ممکن است تسهیلاتی فراتر از اختیار خود (نوشتن) را واپایش کند. به عنوان مثال، ممکن است APP5 فرمان‌ها را به GW2 ارسال کند و تلاش کند دیسک متصل به GW2 را واپایش کند.

Case E– داده‌های ذخیره‌شده در ذخیره‌ساز ممکن است به اشتباه توسط GW ها یا APP ها رونویسی شود. برای مثال، داده‌های ذخیره‌شده در Storage2 ممکن است توسط GW1 یا APP5 رونویسی شود.

Case F- GW ممکن است داده‌ها را به یک Mal-APP بدون دانستن این که آن Mal-APP است بفرستد، که این موضوع در نتیجه افشای داده است.

Case G– یک سیم شناور ممکن است ارتباطات بین مولفه‌ها در سامانه‌های IEEE 1888 را اخذ کند و وضعیت تسهیلات، داده‌های برنامه کاربردی و غیره را استراق سمع کند.

Case H- مهاجم می‌تواند پیام‌های تبادل‌شده میان مولفه‌ها را تغییر دهد و باعث رفتار غیر عمدی تسهیلات شود.

برای یک سامانه جامع IEEE 1888 مستقر و عملیاتی شده، کل زمینه امنیت با در نظر گرفتن مشخصه‌های برنامه‌های کاربردی سامانه IEEE 1888 و پروتکل‌های امنیت بالغ پیچیده و وسیع است. برخی از مسائل امنیتی خارج از دامنه کاربرد این استاندارد به شرح زیر است:

الف- مسائل مربوط به امنیت فیزیکی، مانند سیم بریده‌شده، تخریب افزاره و کارساز با حملات فیزیکی، خاموشی و غیره، باید در طول مرحله استقرار و عملیات در نظر گرفته شود.

ب- نشت[1] کلید گواهی همتا باید تشخیص داده شود و توسط سایر چارچوب‌ها و پروتکل‌ها تجدید شود.

پ- فرض بر این است که هر هستار گواهی‌ای دارد که به شیوه‌ای مناسب / امن توزیع و نگهداری می‌شود. مفروضات توسط سایر چارچوب‌ها و پروتکل‌ها پیاده‌سازی می‌شود.

ت- فرایند اعتماد به محصولات IEEE 1888 باید در موردی که برخی از محصولات ممکن است در زمان خریداری نادرست باشند، توسط یکپارچه‌کنندگان سامانه IEEE 1888 انجام شود.

ث- این ویژگی، رویکرد پیکربندی امنیت لایه انتقال (TLS) مرتبط با پارامترهای امنیتی را توصیف می‌کند. با این حال، برنامه‌های کاربردی مختلف IEEE 1888 باید خودشان محتویات سیاست‌های امنیتی را به عنوان اصالت‌سنجی دو جانبه یا اصالت‌سنجی یک طرفه تعریف و توصیف کند.

ج- انکار خدمت (DoS)[2] و انکار خدمت توزیع شده (DDoS) باید تشخیص داده شود و به طور امن توسط سایر سازوکارها پردازش شود.

1 - Leak
2 - Denial of service

۴-۲ الزامات امنیتی

۴-۲-۱ حفاظت امنیت جامع

توصیه می‌شود امنیت تعریف‌شده در این استاندارد، تمام کارکردها و روش‌های اجرایی پروتکل IEEE 1888 را پوشش دهد، از جمله بازیابی اطلاعات، ذخیره‌سازی اطلاعات، انتقال اطلاعات، استفاده یکپارچه از اطلاعات، واپایش از دور، ثبت نام و غیره.

۴-۲-۲ کارایی بالا با هزینه کم

روش‌ها و پروتکل‌های امنیتی تعریف‌شده در این استاندارد باید هزینه زمان اضافی، مصرف منابع ارتباطی و مصرف منابع محاسباتی را در محدوده معقول و قابل قبول محدود کند.

۴-۲-۳ محرمانگی پیام تبادل IEEE 1888

محرمانگی، خدمت امنیتی است که از داده‌ها در برابر افشای غیر مجاز محافظت می‌کند. هدف حفاظت از اطلاعات در مقابل تهدید غیر فعال است.

۴-۲-۴ یکپارچگی پیام تبادل IEEE 1888

یکپارچگی به معنی محافظت از اطلاعات، داده‌ها و سایر منابع از تغییر ناخواسته در طول روش اجرایی انتقال است. تمامی تغییرات در داده‌ها باید دیده شود. هدف بهبود دقت و کامل بودن اطلاعات و روش‌های پردازش مربوط به حفاظت اطلاعات از تهدید فعال است.

۴-۲-۵ واپایش دسترسی مولفه‌ها

واپایش دسترسی قابلیت درستی‌سنجی حق دسترسی به منابع خاص از یک مولفه خاص را فراهم می‌کند. امنیت IEEE 1888 باید با واپایش دسترسی برای pointID ها در IEEE 1888 که سایر مولفه‌های IEEE 1888 به آن دسترسی دارند، رسیدگی شود.

۴-۲-۶ اصالت‌سنجی متقابل بین مولفه‌ها

درخواست‌ها و پاسخگوهای همسان «همتاها»[1] نامیده می‌شود. اصالت‌سنجی متقابل همتاها را قادر به اصالت‌سنجی یکدیگر می‌کند. امنیت IEEE 1888 باید کارخواه را برای اتصال به کارساز در نظر گرفته شده قادر سازد (به عنوان مثال، ذخیره‌ساز) و کارساز بداند کدام کارخواه (مثلا یک APP) متصل است. این موضوع آنها را از ارسال یا دریافت پیام IEEE 1888 اشتباه بین مولفه IEEE 1888 مخرب یا ناخواسته محافظت می‌کند. در برخی موارد، ممکن است کارساز[2] به کارخواه‌ها[1] اجازه دهد به برخی داده‌ها بدون

1 - Peers
2 - Server

اصالت‌سنجی دسترسی یابد. علاوه بر این، کارخواه نیز ممکن است نیاز به اصالت‌سنجی کارساز داشته باشد. امنیت IEEE 1888 این موارد را بر اساس پیکربندی شان مجاز می‌داند.

۴-۲-۷ اصالت‌سنجی مقیاس‌پذیر و سازوکارهای واپایش دسترسی

امنیت IEEE 1888 باید به انواع مختلفی از سامانه‌های IEEE 1888 اعمال شود به دلیل این که IEEE 1888در انواع گسترده‌ای از مقیاس‌پذیری سامانه و در انواع مختلفی از شکل گیری مدیریت مورد استفاده خواهد گرفت. حتی زمانی که یک سامانه IEEE 1888 میلیون‌ها افزاره را مستقر می‌کند، اصالت‌سنجی و سازوکارهای واپایش دسترسی باید به راحتی مقیاس شود.

۴-۳ اصول طراحی

۴-۳-۱ فناوری‌های موجود برای استفاده مجدد

برنامه‌های کاربردی فناوری‌های امنیتی که به طور گسترده استاندارد و استفاده‌شده، اتخاذ می‌شود. امنیت IEEE 1888 می‌تواند خواص اساسی را با استفاده از واسطهای استاندارد و کتابخانه‌های نرم‌افزاری ارث‌بری کند. از آنجا که IEEE 1888 بر روی پروتکل انتقال ابرمتن (HTTP) طراحی شده است، این استاندارد از HTTP بر اساس TLS (HTTPS) استفاده می‌کند. TLS به طور گسترده‌ای برای اصالت‌سنجی متقابل، یکپارچگی داده‌ها و محرمانگی مورد استفاده قرار می‌گیرد. با اتخاذ HTTPS، IEEE 1888 می‌تواند به راحتی این خواص را بگیرد. برای برآوردن الزامات اصالت‌سنجی، X.509 در این استاندارد به کار گرفته شده است. این موضوع بدین دلیل است که X.509 به طور گسترده‌ای مستقر شده و TLS می‌تواند آن را اداره کند.

۴-۳-۲ مدیریت گواهی جداگانه و کارکرد مدیریت واپایش دسترسی

به منظور برآورده ساختن الزام مقیاس‌پذیری امنیت IEEE 1888، مدیریت گواهی و مدیریت واپایش دسترسی به عنوان کارکردهای مستقل به طور جداگانه در این استاندارد در نظر گرفته شده است.

۴-۳-۳ سازگاری

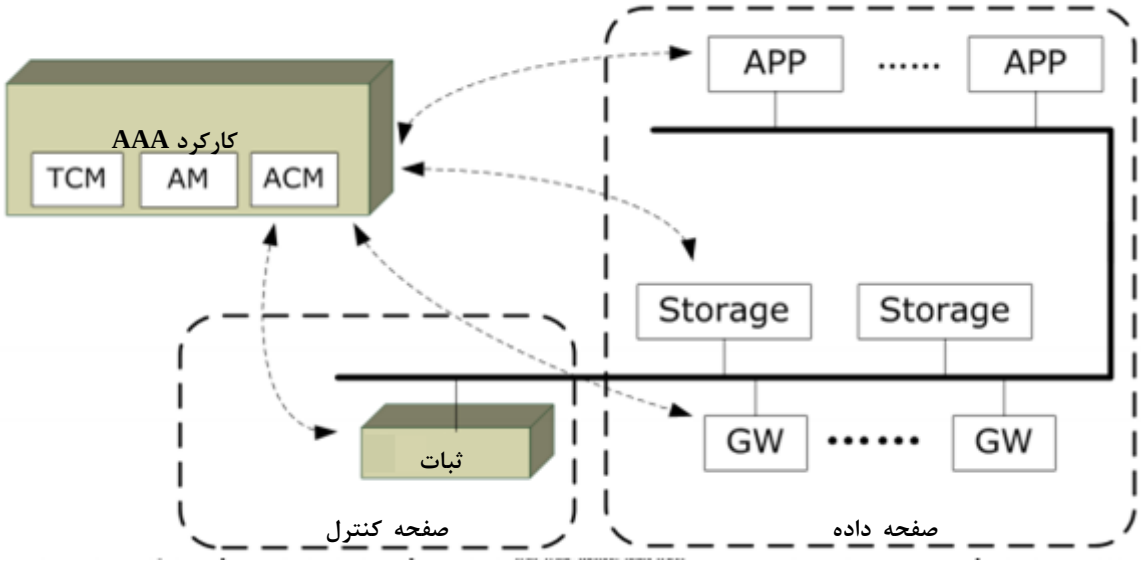
توصیه می‌شود معماری امنیتی تغییرات در معماری IEEE 1888 و هسته‌های کارکردی در کمترین حد ممکن را معرفی کند.

1 - Clients

۵ معماری امنیتی

۵-۱ معماری سامانه

هدف از یک سامانه امنیتی IEEE 1888 محافظت از سامانه IEEE 1888 در برابر تهدیدات امنیتی توصیف‌شده در بند ۴-۱ است. شکل ۲ معماری سامانه امنیتی IEEE 1888 را نشان می‌دهد. سامانه IEEE 1888 TLS (HTTPS به جای HTTP ساده) را برای حفاظت از ارتباطات میان مولفه‌ها و ثبات‌ها اتخاذ می‌کند. سامانه IEEE 1888 باید قبل از شروع روش اجرایی TLS از الزامات برنامه کاربردی آگاه باشد. توصیه می‌شود مولفه‌ها و ثبات‌ها یک گواهی برای شناسایی شناسانه خود (ID ها) در اتصال TLS داشته باشند.



شکل ۲- معماری سامانه امنیت IEEE 1888

همانطور که در شکل ۲ نشان داده شده، مولفه‌های (APP، Storage و GW) و ثبت‌کننده به طور معمول در IEEE 1888 تعریف می‌شود. کارکرد اصالت‌سنجی، مجوزدهی و پاسخگویی (AAA) دارای سه کارکرد است:

مدیر پیکربندی TLS (TCM)[1]، مدیر اصالت‌سنجی (AM)[2] و مدیر واپایش دسترسی (ACM)[3].

TCM پارامترهای پیکربندی TLS را بسته به نرم‌افزار مورد نیاز مدیریت و حفظ می‌کند. TCM برخی پیکربندی‌های TLS، مانند الگوریتم‌های رمزنگاری، طول کلید و غیره (پارامترهایCipherSuite) را به اجرا می‌گذارد. برای جزئیات بیشتر به بند ۶-۳-۱ مراجعه شود.

1 - TLS configuration manager
2 - authentication manage
3 - access control manager

AM دو کارکرد دارد: درستی‌سنجی گواهی (CV)[1] و درستی‌سنجی ID (IV)[2]. CV گواهی ارسال شده از طرف کارخواه TLS یا کارساز TLS را وارسی می‌کند و پاسخ این که آیا گواهی قابل اعتماد است یا خیر را ارائه می‌کند. CV گواهی را بر اساس فهرست اعتماد مجریان از پیش نصب شده در خود درستی‌سنجی می‌کند. IV به اصالت‌سنجی همتا رسیدگی می‌کند. برای جزئیات بیشتر به بند ۶-۳-۲ مراجعه شود.

ACM پاسخ می‌دهد که آیا کارخواه TLS متصل حقوق دسترسی به منابع درخواست شده (به عنوان مثال، روش‌ها و نقاط) را دارد یا خیر. خط‌مشی واپایش دسترسی که در اینجا مدیریت می‌شود، به طور معمول به شکل فهرست واپایش دسترسی از پیش پیکربندی‌شده است. برای جزئیات به بند ۶-۳-۳ مراجعه شود.

۲-۵ آغازگر[3] و پاسخگو[4]

استاندارد IEEE 1888 ، مولفه‌ها و ثبات‌ها را به عنوان هستارهای ارتباطی تعریف می‌کند. با این حال، از نقطه نظر امنیت، توصیه می‌شود پیاده‌سازی‌کنندگان به جای نقش هستارها از مسیر ارتباطی آگاه باشند. بنابراین، هستارها بر اساس مسیر ارتباطاتی و نقش‌های خود در روش اجرایی ارتباط امن طبقه‌بندی شوند. این ویژگی، اصطلاحات جدید «آغازگر» و «پاسخگو» را برای توصیف هستارهای فعال امنیتی IEEE 1888 معرفی می‌کند. این مفهوم مربوط به «کارخواه TLS» و «کارساز TLS» تعریف شده در ویژگی TLS (RFC 5246) است.

- آغازگر، مولفه فعال امنیتی IEEE 1888 (به عنوان مثال، GW، ذخیره‌ساز یا برنامه کاربردی) است که ارتباط TLS را به عنوان نقش کارخواه TLS آغاز می‌کند. برای ارتباط بین مولفه‌ها، آغازگر یک پرس‌وجو یا روش داده در مولفه IEEE 1888 موجود در پاسخگو را فراخوانی می‌کند (به قسمت پایین مراجعه شود). برای ارتباط بین مولفه و ثبات IEEE 1888، آغازگر، ثبت نام یا روش مشاهده در ثبات موجود در پاسخگو را فراخوانی می‌کند.
- پاسخگو مولفه فعال امنیتی یا ثبات IEEE 1888 است که به راه اندازی نشست TLS بین آغازگر پاسخ می‌دهد و درخواست‌های پرس‌وجو / داده یا ثبت نام / مشاهده ارسال شده از آغازگر IEEE 1888 را انجام می‌دهد.

1 - certificate verification
2 - ID verification
3- Initiator
4 - Responder

۵-۳ شناسانه

۵-۳-۱ چگونگی اختصاص شناسانه (ID) برای هستارهای IEEE 1888

خود مولفه یا ثبات اصلی IEEE 1888 (بعد از این، برای سادگی «هستار» گفته می شود) ID ندارد و تنها یک شناسانه منبع یکنواخت دسترسی (URI) در فضای اینترنت دارد. در مضمون امنیت IEEE 1888، هر مولفه و ثبات باید یک ID برای شناسایی خود برای اصالت‌سنجی با یکدیگر داشته باشد و واپایش دسترسی همتا را در سمت کارساز فعال کند. این ویژگی قواعد زیر را برای تخصیص یک شناسه برای هر هستار IEEE 1888 تعریف می‌کند.

- آغازگر و پاسخگو باید تنها یک مولفه یا ثبات IEEE 1888 باشد.
- آغازگر یا پاسخگو باید یک نام منحصر به فرد جهانی داشته باشد و نام خود را در بخش نام جایگزین موضوع (SAN) در قالب گواهی X.509 (بخش ۴-۲-۱-۶ RFC 5280) جای دهد. این نام منحصر به فرد جهانی یک ID است.

۵-۳-۲ قالب نام جایگزین موضوع (SAN)

قالب SAN از هر نوع گواهی به شرح زیر است:

- گواهی با **نقش-میزبان** باید نام دامنه کاملا واجد شرایط ID را در قالب (FQDN) (به RFC 1035 مراجعه شود) یا نشانی نسخه ۴ پروتکل اینترنت (IPv4) (به RFC 791 مراجعه شود) یا نسخه ۶ پروتکل اینترنت (IPv6) (به RFC 2460 مراجعه شود) داشته باشد. ID در SAN تنها ذخیره می‌شود (به عنوان مثال، (type:2 - dNSName) (به بخش ۴-۲-۶-۱ RFC 5280 مراجعه شود). URI دسترسی پاسخگو باید FQDN یا نشانی پروتکل اینترنت (IP) را شامل شود. علاوه بر این، اگر IDاز قالب FQDN استفاده کند، باید توسط برخی سامانه‌های وضوح نام به طور معمول توسط سامانه نام دامنه (DNS) حل و فصل شود.
- **گواهی با نقش کارخواه** باید یک ID در قالب رایانامه داشته باشد (به بخش ۳-۴-۱ RFC 5322 مراجعه شود) و ID را در SAN تنهای خود ذخیره کند (به عنوان مثال، type:1- rfc822Name (به بخش-۴-۲-۱-۷ RFC 2459 مراجعه شود). نشانی رایانامه نباید قابل دسترسی باشد (به عنوان یک نشانی رایانامه)

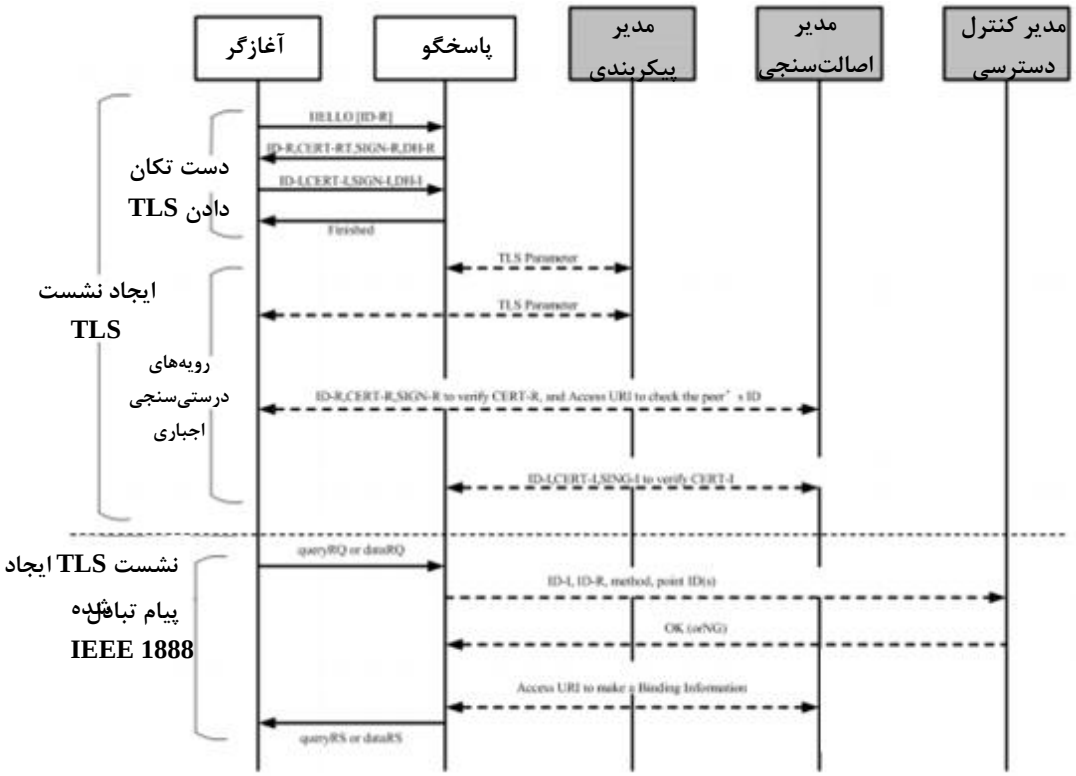
۵-۳-۳ شناسانه (ID) «ناشناس»

اگر یک مولفه نمی‌تواند شناسایی شود، مولفه می‌تواند به عنوان مولفه‌ای که ID «ناشناس» دارد، رسیدگی شود. به عبارت دیگر، شناسه «ناشناس» محفوظ نگه داشته شده است و نباید به عمد به هیچ مولفه‌ای تخصصیص داده شود.

۶ پروتکل‌های امنیتی

۶-۱ دنباله ارتباطی

دنباله ارتباطی میان مولفه‌ها، ثبات و کارکردهای IEEE 1888 AAA، (شکل ۳) در اینجا توصیف شده است. هستارهای IEEE 1888 که از امنیت پشتیبانی می‌کند (از جمله آغازگر و پاسخگو) با کارکردهای AAA توصیف‌شده در ۵-۱ تعامل می‌کند (برای جزئیات بیشتر در تعریف کارکردهای AAA، به بند ۶-۳ مراجعه شود.)



شکل ۳- دنباله ارتباطی

شکل ۳ دنباله ارتباطی را بین این آغازگرها، پاسخگوها، مدیر پیکربندی TLS، AM و .ACM نشان می‌دهد. ارتباط تقریبا شامل دو مرحله است:

- استقرار نشست TLS
- تبادل پیام IEEE 1888

مرحله اول به صورت منطقی به دو قسمت تقسیم می‌شود. قسمت اول «دست‌دهی[1] TLS» شامل ایجاد یک نشست TLS. دست‌دهی باید با RFC 5246 مطابقت داشته باشد. قسمت دوم «روش‌های اجرایی درستی‌سنجی اجباری» که شامل سه روش اجرایی زیر است:

الف- وارسی پارامترهای اتصال برای نشست TLS ایجادشده

ب- درستی‌سنجی گواهی از همتا

پ- شناسایی و اصالت‌سنجی همتا

این ویژگی، ترتیب این روش‌های اجرایی را در مرحله اول تعریف نمی‌کند. به عنوان مثال، پاسخگو می‌تواند AM را (این یکی از روش‌های اجرایی درستی‌سنجی الزامی است) در طول قسمت دست‌دهی TLS پرس و جو کند. هر دو آغازگر و پاسخگو باید تمام روش‌های اجرایی را قبل از ایجاد نشست TLS اجرا کنند. در مرحله دوم، پاسخگو، اجازه دسترسی آغازگر به ACM را پرس‌وجو می‌کند.

گواهی‌های تبادل‌شده بین آغازگر و پاسخ در طول شروع نشست TLS ممکن است به طور امن در «ذخیره‌ساز کلید» در هر دو طرف نصب شده باشد. ذخیره‌ساز کلید به طور معمول در آغازگر و ارائه‌دهنده محلی، به عنوان مثال، در فایل ذخیره‌ساز کلید پیاده‌سازی می‌شود. با این حال، یک پیاده‌سازی احتمالی دیگر ذخیره‌ساز کلید می‌تواند کارت هوشمند باشد؛ کاربران ممکن است کلیدهای خود را در کارت هوشمند دارا باشند و از گواهی‌های خود برای AAA استفاده کنند.

این ویژگی در واقع طرح اصالت‌سنجی بین کاربران و مولفه‌های IEEE 1888 را تعریف نمی‌کند. این موضوع بدین دلیل است که تعامل بین کاربر و مولفه باید در واسط کاربر (UI) ایجاد شود و خارج از دامنه کاربرد IEEE 1888 است. برخی از پیاده‌سازی‌ها اصالت‌سنجی نام‌کاربری/ رمز عبور را در UI می‌خواهد و برخی دیگر اصالت‌سنجی مبتنی بر کارت هوشمند را فقط همان طور که در بالا توضیح داده شده می‌خواهد. اگر پیاده‌سازی‌کنندگان امنیت نیاز به واپایش کاربران با توجه به نقش آنها برای سامانه IEEE 1888 داشته باشند، یکی از پیاده‌سازی‌ها موارد زیر خواهد بود:

الف- آماده‌سازی چند شناسانه (به بند ۵-۳ مراجعه شود) که نشان دهنده نقش کاربران است

ب- ایجاد اصالت‌سنجی کاربران در امنیت UI

پ- نگاشت کاربر به ID مربوط، نقش و خط‌مشی دسترسی که درکارکردهای AAA مدیریت می‌شود.

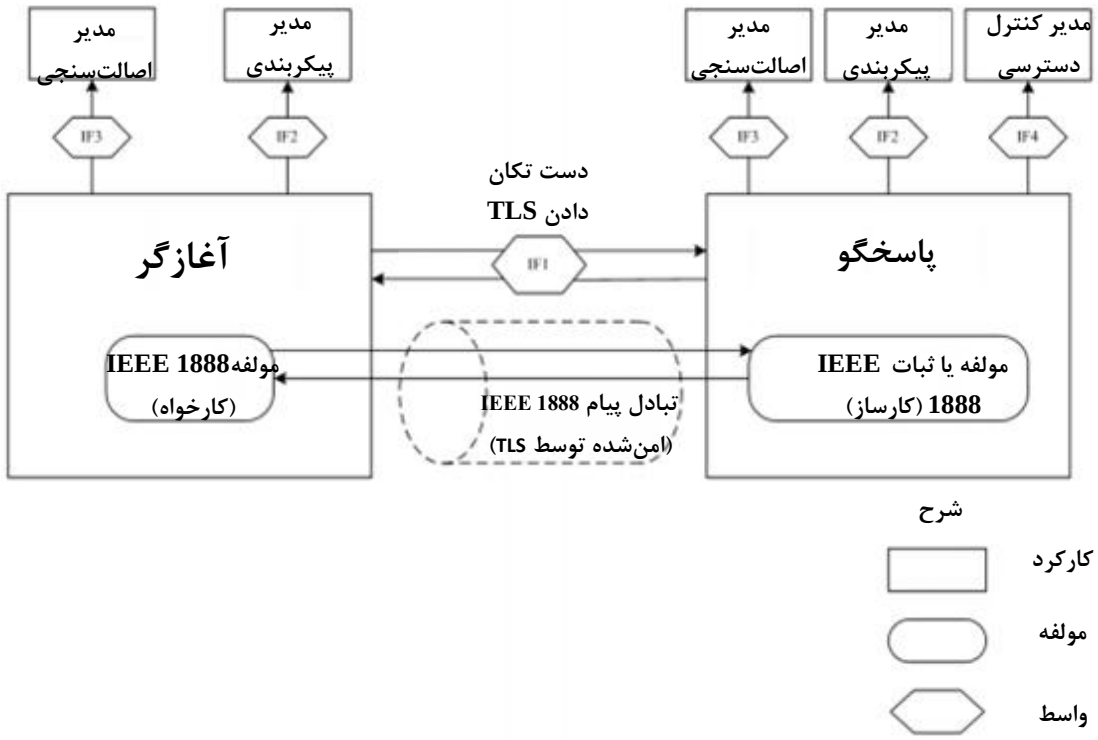
در این روش، امنیت IEEE 1888 به طور غیر مستقیم اصالت‌سنجی، مجوزدهی و واپایش دسترسی کاربر را امکان‌پذیر می‌کند.

1 - Handshake

شکل ۳ تنها مورد موفقیت اصالت‌سنجی متقابل بین آغازگر و پاسخ را نشان می‌دهد. اگر این سامانه به اصالت‌سنجی متقابل به عنوان خط‌مشی امنیتی خود نیاز داشته باشد، نشست TLS اگر یکی از CV ها یا اصالت‌سنجی‌ها شکست بخورد، باید قبل از تبادل پیام‌های IEEE 1888 پایان یابد. به عنوان مثال اگر سامانه IEEE 1888 اصالت‌سنجی یک طرفه یا هیچ اصالت‌سنجی را به عنوان خط‌مشی‌های امنیتی خود اجازه نمی‌دهد، این روش اجرایی ممکن است ادامه یابد. برای اطلاعات بیشتر به بند ۶-۳-۲ مراجعه شود.

۶-۲ تعریف واسط

معماری نرم‌افزار امنیت IEEE در اینجا توصیف شده و تعریف واسط‌ها با جزئیات بیشتر ارائه شده است (شکل ۴)



شکل ۴- معماری نرم‌افزار امنیت فعال واسط‌های IEEE 1888

۶-۲-۱ IF1: دست‌دهی TLS

IF1 یک واسط بین آغازگر و پاسخگو است که پارامترهای TLS برای ایجاد یک کانال امن را که از پیام IEEE 1888 محافظت می‌کند، ایجاد می‌کند. امنیت IEEE 1888، TLS را برای IF1 وارد می‌کند، در نتیجه پیاده‌سازی‌کننده باید سازوکار TLS را اعمال کند.

از آنجا که این ویژگی نیاز به اصالت‌سنجی متقابل بین آغازگر و پاسخگو دارد، پاسخگو باید پیام گواهی کارساز تعریف شده توسط بخش ۷-۴-۲ RFC 5246 را ارسال کند و همچنین باید ارسال پیام درخواست

گواهی تعریف شده توسط بخش ۷-۴-۴ RFC 5246 را ارسال کند. اگر آغازگر قصد ندارد که کارساز دسترسی کارخواه را به عنوان یک ناشناس رسیدگی کند، توصیه می‌شود آغازگر پیام گواهی کارخواه تعریف شده توسط بخش ۷-۴-۶ RFC 5246 را ارسال کند. اگر آغازگر هیچ گواهی‌ای را ارسال نکند، پاسخگو نباید آن را به عنوان یک هشدار واکشی handshake_failure رسیدگی کند و باید به دست‌دهی ادامه دهد و مشتری را به عنوان ناشناس تعیین کند.

آغازگر باید پسوند نشانه نام کارساز (به RFC 6066 مراجعه شود) را به منظور پشتیبانی از چندین نمونه مولفه که یک نشانی IP واحد را به اشتراک می‌گذارد، ارسال کند (به عنوان مثال، VirtualHost)

۶-۲-۲ IF2: پیکربندی TLS

IF2 واسط بین مدیر پیکربندی TLS و آغازگر / پاسخگو است. آغازگر باید پارامترهای TLS پشتیبانی‌شده را پرس و جو کند. پاسخگو باید پارامترهای اتصال TLS، مانند مجموعه رمز دریافت شده از اتصال همتای از دور را به TCM ارسال کند. TCM باید جواب قبول یا رد ارتباط را بدهد.

IF2 ممکن است «پارامترهای اتصال همتای خاص» را ارائه دهد. آغازگر/ پاسخگو ممکن است داده‌های فرعی (به عنوان مثال شناسانه همتا، URI دسترسی و غیره) را ارسال کند. پس از آن، TCM به پارامترهای اتصال TLS (به عنوان مثال الگوریتم رمزنگاری، طول کلید و غیره) مربوط به داده‌های فرعی داده شده پاسخ می‌دهد.

این ویژگی، یک پروتکل دقیق، واسط یا پارامترهای قابل تنظیم برای پیکربندی مشخص می‌کند. بسته به الزامات سامانه، از جمله عملکرد، مقیاس سامانه و طرح عملیات، معماری امنیتی IEEE 1888 باید سبک‌های مختلف پیاده‌سازی استفاده شود. برای مثال،

الف- پیاده‌سازی بر اساس فایل برای سامانه‌های مقیاس کوچک موثر کار می‌کند.

ب- پیاده‌سازی مبتنی بر کارساز ممکن است هزینه‌های عملیات مدیریت پیکربندی TLS برای سامانه‌های مقیاس بزرگ را کاهش دهد.

۶-۲-۳ IF3: اصالت‌سنجی

IF3 واسط بین AM و آغازگر / پاسخگو است IF3 موارد زیر را ارائه می‌کند:

- کارکرد CV
- کارکرد IV

برایC ، آغازگر / پاسخگو باید فهرستی از زنجیره گواهی از گواهی همتا (به عنوان مثال، گواهی برای آغازگر یا پاسخ) را ارسال کند. پس از آن، AM باید به نتیجه اعتبارسنجی پاسخ دهد. این ویژگی هیچ پروتکلی برای تبادل پارامترها را مشخص نمی‌کند. توصیه می‌شود پیاده‌سازی‌کننده از پروتکل وضعیت گواهی برخط

(OCSP) (به RFC 627 مراجعه شود) یا ماژول (پودمان) اعتبارسنجی جاسازی شده غیر برخط، همچون OpenSSL استفاده کند.

برای IV، تنها آغازگر باید موارد زیر را ارسال کند:

- ID پاسخگو در SAN گواهی پاسخگو
- FQDN (یا نشانی IP) همتای اتصال، به عنوان مثال، قسمت میزبان URI دسترسی

AM آنها را با مراجعه به حافظه انقیاد مقایسه می‌کند تا وجود ID در حافظه اطلاعات انقیاد را درستی‌سنجی کند. AM باید نتیجه IV را پاسخ دهد.

این ویژگی پروتکل دقیق یا واسط کاربری برای CV و IV را مشخص نمی‌کند. بسته به نوع الزامات سامانه، از جمله عملکرد، مقیاس سامانه و طرح عملیات، معماری امنیت IEEE 1888 باید سبک‌های مختلف پیاده‌سازی را استفاده کند. به طور مثال

الف- پیاده‌سازی بر اساس فایل برای سامانه‌های مقیاس کوچک موثر کار می‌کند.

ب- پیاده‌سازی مبتنی بر کارساز ممکن است هزینه‌های عملیات مدیریت پیکربندی و عملیات مدیریت ID برای سامانه‌های مقیاس بزرگ را کاهش دهد.

۶-۲-۴ IF4: واپایش دسترسی

IF4 واسط بین ACM و پاسخگو است. پاسخگو از آغازگر به ACM درخواست اجازه می‌کند (چه به درخواست آغازگر مجاز باشد چه خیر). پس از آن، ACM پاسخ نتیجه را می‌دهد. در این ویژگی، کمینه، پارامترهای زیر باید از طریق IF4 تبادل شود:

- ID آغازگر
- ID پاسخگو
- فهرست pointID های هدف
- نام روش (به عنوان مثال، پرس و جو / داده / ثبت نام / مشاهده)
- نوع پرس و جو (به عنوان مثال، ذخیره‌سازی / جریان) اگر روش پرس و جو است

فهرست زنجیره گواهی ممکن است به صورت اختیاری اضافه شده باشد. فهرست زنجیره گواهی اجازه گروه را می‌دهد. ACM ممکن است از مرجع صدور گواهی میانی (CA) برای قضاوت حق دسترسی آغازگر استفاده کند. به عنوان مثال، می‌تواند به هر آغازگر امضاشده توسط CA خاص اجازه دهد.

بسته به خط‌مشی‌های امنیتی، کاروَرهای[1] سامانه سایر اطلاعات را برای واپایش دسترسی به کار می‌برند (به عنوان مثال، نشانی IP آغازگر). با این حال، به دلیل این که هدف امنیت IEEE 1888 فعال کردن «واپایش دسترسی بر اساس مولفه IEEE 1888 است. این اطلاعات اضافی اختیاری در این ویژگی باقی می‌ماند. این اطلاعات اختیاری می‌تواند شامل موارد زیر باشد:

- نشانی IP آغازگر (برای واپایش دسترسی IP)
- نتیجه مشاهده معکوس DNS از نشانی IP (برای واپایش دسترسی توسط ناحیه DNS یا نام میزبان)
- زمان مقادیر (برای واپایش دسترسی بر اساس زمان دسترسی)
- زمان مقادیر (برای واپایش دسترسی بر اساس زمان سنجش)
- فهرست componentID های هدف اگر روش، ثبت نام است

این ویژگی پروتکل دقیق یا واسط کاربری برای درستی‌سنجی واپایش دسترسی را مشخص نمی‌کند. بسته به الزامات سامانه، از جمله عملکرد، مقیاس سامانه و طرح عملیات، معماری امنیت IEEE 1888 باید سبک‌های مختلف پیاده‌سازی را استفاده کند. به طور مثال

الف- پیاده‌سازی بر اساس فایل برای سامانه‌های مقیاس کوچک موثر کار می‌کند.

ب- پیاده‌سازی مبتنی بر کارساز ممکن است هزینه‌های عملیات مدیریت ACL برای سامانه‌های مقیاس بزرگ را کاهش دهد.

۶-۳ تعریف کارکرد اصالت‌سنجی، مجوزدهی و پاسخگویی (AAA)

۶-۳-۱ مدیر پیکربندی TLS (TCM)

مدیر پیکربندی TLS (TCM)، پارامترهای اتصال قابل تنظیم TLS را مدیریت می‌کند. به طور مثال، TCM ممکن است از الگوریتم رمزنگاری خاص برای هر اتصال یا یک اتصال خاص که توسط شناسانه‌های همتا یا URI دسترسی و غیره را دسته‌بندی می‌کند، استفاده کند.

TCM باید دو کارکرد زیر را ارائه دهد:

- برای آغازگر (کارخواه TLS) مجموعه پارامترهای نامزد TCM را ارائه کند.
- برای پاسخگوها (کارساز TLS) TCM اجازه دهد تا مجموعه پارامترهای داده شده را از آغازگر همتا ارتباطاتی (کارخواه TLS) رد کند.

TCM ممکن است کارکردی که پارامتر اتصال را برای ID همتا داده شده است از یک نام دامنه یا نشانی IP بازگرداند.

1 - Operators

۶-۳-۲ مدیر اصالت‌سنجی (AM)

AM باید دست کم دو کارکرد ارائه دهد: CV و IV. CV اجازه می‌دهد تا آغازگر و پاسخگو وارسی کنند که گواهی داده شده از همتای از دور معتبر است یا خیر. توصیه می‌شود رفتار اساسی برای این CV توسط RFC 5280 هدایت شود. نقش IV شناسایی پاسخگو است. به عنوان مثال، IV اتصال آغازگر به همتای درست را امکان‌پذیر می‌کند. به منظور درستی‌سنجی هویت پاسخگو، IV در AM (در سمت آغازگر) باید

الف- IDمشخص شده در SAN گواهی پاسخگو را با FQDN یا نشانی IP همتا مقایسه کند، یا

ب- حافظه اطلاعات انقیاد را مشاهده کند (به بند ۶-۳-۲-۲ مراجعه شود)

۶-۳-۲-۱ همتای ناشناس[1]

سامانه IEEE 1888 ممکن است اتصال‌هایی که نمی‌تواند اصالت‌سنجی شود را رد کند. با این حال، ممکن است مولفه چنین اتصال‌هایی را به برخی دلایل قبول کند. به عنوان مثال، حسگر محدودیت که نمی‌تواند TLS را اجرا کند می‌خواهد داده‌های خود را در ذخیره‌ساز بنویسد و ذخیره‌ساز می‌خواهد به آن اجازه دهد. بنابراین، سامانه امنیتی فعال IEEE 1888 ممکن است خط‌مشی‌های امنیتی را به عنوان اجازه به اتصال بدون اصالت‌سنجی همتا در موارد زیر پیکربندی کند:

اتصال از TLS (HTTP خام) استفاده نمی‌کند.

اتصال از TLS، استفاده می‌کند اما آغازگر گواهی کارخواه خود را ارسال نمی‌کند.

در این مورد، همتا باید به عنوان مولفه‌ای که ID آن «ناشناس» است، رسیدگی شود که در بخش ۶-۳-۳ تعریف شده است و پاسخگو باید به ACM برای اتصال همتا مشاوره دهد.

۶-۳-۲-۲ پاسخگو با گواهی با نقش کارخواه

گواهی با نقش کارخواه اساسا برای استفاده آغازگر در نظر گرفته شده است. به عنوان مثال، مولفه‌ای که گواهی با نقش کارخواه دارد داده‌ها را تنها از ذخیره‌ساز بازخوانی می‌کند، پس از آن داده‌ها را تحلیل می‌کند و آن را برای کاربران مصور می‌کند. به عبارت دیگر، زمانی که پاسخگو از گواهی با نقش کارخواه استفاده می‌کند، مشکل وجود دارد.

برای آغازگر، اصالت‌سنجی پاسخگو با مقایسه ID در SAN گواهی پاسخگو، به قسمت میزبان URIدسترسی پاسخگو در مورد نمونه استفاده از TLS انجام می‌شود. با این حال، ID گواهی با نقش کارخواه به عنوان FQDN یا نشانی IP قالب‌بندی نمی‌شود. آغازگر نمی‌تواند پاسخگو را به این روش زمانی که پاسخگو دارای گواهی با نقش کارخواه است، اصالت‌سنجی کند.

1 - Anonymous

به منظور حل این مشکل، این ویژگی، مفهوم معرفی «اطلاعات انقیاد» را معرفی می‌کند.

اطلاعات انقیاد، ارتباط ID گواهی با نقش کارخواه پاسخگو با URI دسترسی برای پاسخگو همراه با طول عمر باقی مانده این ارتباط است.

این ویژگی همچنین به معرفی مفهوم «حافظه اطلاعات انقیاد» می‌پردزاد که اطلاعات انقیاد را در AM نگه می‌دارد.

اطلاعات انقیاد به طور مفهومی حوزه‌های زیر را شامل می‌شود:

- ID گواهی با نقش کارخواه برای پاسخگو (بالقوه)
- URI دسترسی پاسخگو که از گواهی با نقش کارخواه بالا استفاده می‌کند
- مقدار طول عمر که عمر باقی مانده برای این اطلاعات را نشان می‌دهد

اگر کاروَر بخواهد به مولفه‌ای که از گواهی با نقش کارخواه استفاده می‌کند اجازه تبدیل شدن به پاسخگو دهد، کاروَر باید اطلاعات انقیاد پاسخگو را فراهم کند. روش فراهم آوردن این اطلاعات انقیاد برای مولفه‌ها یا ثبات‌ها، موضوع محلی پیاده‌سازی است.

آغازگر باید نشست TLS را زمانی که ID پاسخگو و URI دسترسی منطبق با ورود اطلاعات انقیاد در حافظه اطلاعات انقیاد است، قبول کند. هنگامی که عمر اطلاعات انقیاد منقضی می‌شود، مولفه باید ورود را از حافظه اطلاعات انقیاد خود حذف کند.

به عنوان مثال، فرض کنید که مولفه X می‌تواند از طریق URI دسترسی "https://TEST.EXAMPLE.COM/" قابل دسترسی باشد، اما X دارای گواهی با نقش کارخواه باشد و ID آن در SAN برابر با X@EXAMPLE.COM باشد و مؤلفه Y (آغازگر) می‌خواهد به مولفه X متصل شود (پاسخگو) و کاروَر این مورد را تا 2012-12-31T00: 00: 00 + 00: 00 اجازه می‌دهد. در این مورد، کاروَر باید Y (آغازگر) را با "until: 2012-12-31T00: 00: 00 + 00: 00”, "https://TEST.EXAMPLE.COM/", "X@EXAMPLE.COM"> ارائه دهد.

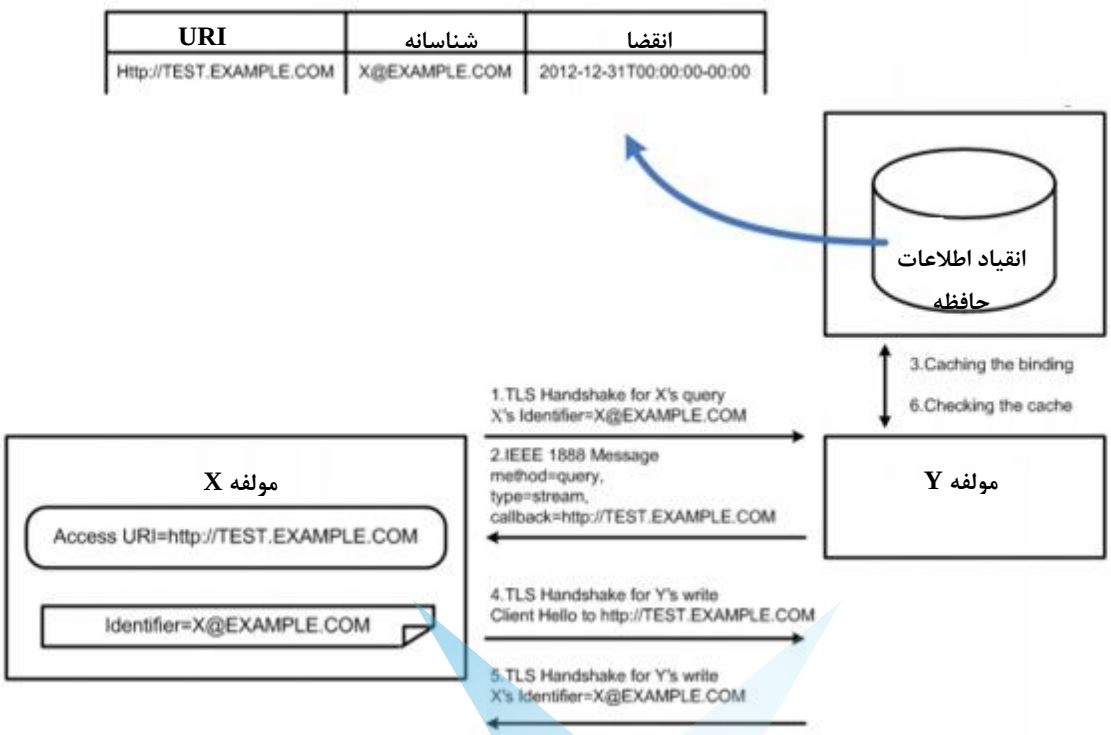
هنگامی که آغازگر Y به X متصل می‌شود، به عنوان مثال، https://TEST.EXAMPLE.COM/، Y، identifier="X@EXAMPLE.COM" را دریافت می‌کند. در مورد نمونه، این نشست در TLS اصالت‌سنجی نشده است چرا که شناسه ("X@EXAMPLE.COM") با قسمت میزبان URI دسترسی ("TEST.EXAMPLE.COM") مطابقت ندارد. با این حال، در حال حاضر Y اطلاعات انقیاد را "2012-12-31T00: 00: 00 + 00: 00, "https://TEST.EXAMPLE.COM/", "X@EXAMPLE.COM"> در حافظه اطلاعات انقیاد خود دارد، بنابراین Y این نشست را می‌پذیرد.

۶-۳-۲-۳ آغازگر با گواهی با نقش کارخواه و پروتکل TRAP

IEEE 1888 پروتکل TRAP را که از ارائه‌دهنده برای انجام پروتکل WRITE به یک مولفه مشخص شده (به نام «تماس بازگشت») در شرایط خاص درخواست می‌کند، ارائه می‌کند. TRAP همچنین به درخواست‌کننده و مولفه تماس برگشت اجازه می‌دهد که مولفه یکسان باشند. این بدان معنی است که درخواست کننده، آغازگر پروتکلTRAP، می‌تواند بعدا یک پاسخگو باشد. در این مورد، ارائه‌دهنده نیاز به اطلاعات انقیاد برای درخواست‌کننده دارد. این ارتباط یک ارتباط پویا است، در نتیجه مدیریت آن توسط کاروَرها امکان‌پذیر است.

به منظور پرداختن به این مشکل، این ویژگی روش اجرایی زیر را معرفی می‌کند. هنگامی که ارائه دهنده درخواست TRAP را می‌گیرد و درخواست‌کننده از گواهی با نقش کارخواه استفاده می‌کند، توصیه می‌شود ارائه‌دهنده اطلاعات انقیاد خود را برای درخواست‌کننده با عمری برابر با زمان اعتبار جستجو [زمان وجود (TTL)] در انقضای درخواست TRAP ایجاد کند. این روش اجرایی «به روز رسانی اطلاعات اتصال پویا» نامیده می‌شود.

علاوه بر این، ارائه دهنده ممکن است اطلاعات انقیاد را "BY_TRAP" نشانه‌گذاری کند و ارائه دهنده اجرا کند که اطلاعات انقیاد مشخص شده فقط برای پروتکل WRITE که توسط پروتکل TRAP ایجادشده، استفاده می‌شود. ارائه دهنده ممکن است نقاط درخواست شده توسط TRAP را به یاد داشته باشد و تایید کند که تمام نقاط در درخواست WRITE که ارائه دهنده ارسال می‌کند در نقاطی که در پروتکل TRAP درخواست‌شده وجود دارند.



شکل ۵ - مثال اطلاعات انقیاد

به عنوان مثال، فرض کنید که مولفه X می‌تواند از طریق URI دسترسی "https://TEST.EXAMPLE.COM/" قابل دسترسی باشد، اما X دارای گواهی با نقش کارخواه با ID خود در SAN "X@EXAMPLE.COM" باشد و مولفه X درخواست TRAP را با مخاطبین callback= "https://TEST.EXAMPLE.COM/"و "point=”/foo/bar به مولفه Y می‌فرستد. مولفه Y این درخواست را دریافت می‌کند و به‌روزرسانی اطلاعات انقیاد پویا را انجام می‌دهد، به عنوان مثال، مولفه Y اطلاعات انقیاد <"X@EXAMPLE.COM", "https://TEST.EXAMPLE.COM/", “until the TRAP expires”> را (توسط TTLدر درخواست) ایجاد می‌کند که به عنوان <" BY_TRAP "در حافظه اطلاعات انقیاد خود علامت‌گذاری شده است. زمانی که مقدار نقطه "/foo/bar" به روز شد، Y شروع به آغاز نشست TLS برای درخواست WRITE به X می‌کند، به عنوان مثال، http://TEST.EXAMPLE.COM/ و Y گواهی X را با "identifier=X@EXAMPLE.COM"دریافت می‌کند. در یک مورد نمونه، این نشست در TLS اصالت‌سنجی نمی‌شود چرا که شناسانه ("X@EXAMPLE.COM") با قسمت میزبان URI دسترسی ("TEST.EXAMPLE.COM" مطابقت ندارد.

با این حال، Y تشخیص داده که اطلاعات انقیاد علامت‌گذاری شده به عنوان "BY_TRAP" وجود دارد و گام بعدی را انجام می‌دهد، Y موارد زیر را تایید می‌کند:

الف- هدف از این نشست ارسال درخواست WRITE ناشی از پروتکل TRAP است

ب- نقطه "/foo/bar" که مقدار آن ارسال می‌شود در درخواست TRAP مولفه X شامل شده

اگر نشست برای درخواست WRITE ناشی از TRAP نباشد که توسط X@EXAMPLE.COM درخواست شده، یا نقطه "/foo/bar" در درخواست TRAP شامل نشده باشد، Y باید نشست را پایان دهد.

۶-۳-۳ مدیر واپایش دسترسی (ACM)

ACM، ACL را با پارامترهای ارسال شده از طریق واسط تعریف‌شده در بند ۶-۲-۴ مقایسه می‌کند.

ACM، قبول یا انکار را برای هر درخواست بازمی‌گرداند.

۶-۴ رد[1] اتصال

امنیت IEEE 1888 دارای دو سطح از رد اتصال است:

الف- بی نتیجه ماندن دست‌دهی TLS

ب- رد سطح IEEE 1888 (با پیغام خطای بند ۶-۴-۱)

1 - Rejecting

آغازگر باید دست‌دهی TLS را در صورت تشخیص هر گونه خطا در طول دست‌دهی TLS بی نتیجه بگذارد و باید با ارسال هشدار خطای TLS به دنبال تعریف بخش ۷-۲-۲ در RFC 5246 باشد، (که در دامنه کاربرد این استاندارد نیست). آغازگر باید هیچ گونه پیام خطا IEEE 1888 را ارسال نکند و باید اتصال را در صورت تشخیص هر گونه خطا و پس از دست‌دهی TLS ببندد.

پاسخ ممکن است دست‌دهی TLS را در صورت تشخیص هرگونه خطا در طول ایجاد نشست TLS بی نتیجه بگذارد و پاسخگو باید با ارسال هشدار خطای TLS از تعریف بخش ۷-۲-۲ در RFC 5246 تبعیت کند، (که در دامنه کاربرد این استاندارد نیست). اگر پاسخگو دست‌دهی TLS را بی نتیجه نمی‌گذارد، باید به پیام درخواست IEEE 1888 از آغازگر گوش دهد اما باید با خطاها در پاسخ IEEE 1888 آنها را رد کند. خطاها باید از تعریف ۶-۴-۱ تبعیت کند.

۶-۴-۱ پیام‌های خطا

پیغام خطا باید یک پیام پاسخ معتبر IEEE 1888 باشد. این پیام باید تنها یک سرایند با یک شی خطا باشد و هر گونه نهاد ارائه شده باید نادیده گرفته شود.

رشته متن برای صفت «نوع» در یک شی خطا در جدول ۱ خلاصه شده است. همچنین توصیه می‌شود دلیل با جزییات قابل خواندن برای انسان در عنصر متن شی خطا گنجانده شود.

جدول ۱ - نوع خطا و توصیف دلیل

نوع	دلیل
اصالت‌سنجی	CV گواهی همتا را رد کرده است.
مجوزدهی	ACM گواهی همتا را رد کرده است.
TLS	TCM گواهی همتا را رد کرده است.
سایر موارد	دیگر قادر به پذیرفتن اتصال به دلایل دیگر نیست.