چارچوب اعتبارسنجی برای اینترنت اشیاء

چکیده

این مقاله یک چارچوبی ارائه میدهد که اجازه کنترل دسترسی fine grain و انعطاف پذیر به دستگاه های متصل بهم با قدرت پردازش و حافظه بسیار محدود میدهد.

مجموعه ای از نیازمندی های امنیتی و اجرایی برای این تنظیمات پیشنهاد شده و یک چارچوب اعتبارسنجی با توزیع هزینه های پردازشی بین دستگاه محدود و سرورهای less constrained بک اند در حالی که تبادل پیام با دستگاه های محدود حداقل بماند، از آن استنتاج میشود.

برای اثبات این مفهوم ما نتایج پیاده سازی یک نمونه اولیه با اجرای بخشی از این چارچوب را ارائه میکنیم.

کلمات کلیدی: اینترنت اشیاء، کنترل دسترسی، اثبات

1. معرفی

اینترنت اشیاء (IoT) یک اصطلاح معمول مورد استفاده برای توصیف یک جامعه از شبکه هاست که در آن همه چیز در آن می توانند با اتصال به هم نفع ببرند. این به آن معنی است که برخلاف گذشته که در آن تلفن های همراه و کامپیوترها بطور سراسری از طریق اینترنت بهم پیوستند، امروزه انواع تجهیزات الکترونیکی به صورت آنلاین در آمده اند. انتظار می رود سرعت این روند در سالهای آینده با توجه به کاهش هزینه های سخت افزاری و شبکه و همچنین بلوغ تکنولوژی اینترنت شتاب پیدا کند.

در این مقاله ما به یکی از چالش های مهم امنیتی، اعتبارسنجی و کنترل دسترسی از نظر سیستمهای متصل متشکل از دستگاه های با منابع محدود می پردازیم که به طور مستقیم توسط انسان اداره نمی شوند. به طور

خاص، روی مساله ای تمرکز میکنیم که در آن یک دستگاه محدود با چند دستگاه دیگر و یا با کامپیوترهای بک اند ارتباط دارد.

این به معنی این است که حتی اگر دستگاه ابتدا توسط یک فرد یا سازمان پیکربندی شده باشد، باید قادر به برقراری ارتباط با سایر نهادها باشد و این نهادهای مختلف ممکن است از حقوق دسترسی یکسان برخوردار نباشند، به عنوان مثال، این دستگاه باید قادر به تمایز بین درخواست ها از سازمان های مختلف و اجرای تصمیمات اعتبارسنجی fine-grained باشد.

علاوه بر این، اجازه می دهیم که تصمیمات اختیاردهی مربوط به یک دستگاه براساس اطلاعات محلی تنها در دسترس خود دستگاه باشند. استفاده از شرایط دستگاه محلی برای سیاست تصمیم گیری، انعطاف پذیری قابل توجهی را به مدل های کنترل دسترسی قابل پشتیبانی می افزاید، از آنجا که هر پارامتر خوانده شده توسط دستگاه را می توان در شرایط اعطای یک درخواست مورد استفاده قرار داد.

هدف این مقاله، حمایت از روشهای عمومی مجوز و کنترل دسترسی قابل اعمال در انواع دستگاه ها و اهداف دسترسی است. با این حال، از آنجا که دستگاه های محدود عامل محدود کننده هستند، باید بدترین حالت را فرض کرده و با محاسبات و بودجه ارتباطاتی محدود طراحی نماییم (ارسال و دریافت پر هزینه ترین اعمال برای دستگاه های حسگر بی سیم شناخته شده اند).

سهم ما در این مقاله یک چارچوب اعتبارسنجی عمومی با قابلیت پشتیبانی از کنترل دسترسی ریز دانه و انعطاف پذیر برای دستگاه های محدود با خصوصیات زیر است:

- دستگاه تصمیم های کنترل دسترسی به صورت محلی میگیرد؛
- تصمیمات ممکن است بر اساس پارامترهای محلی دستگاه گرفته شوند؛
- چارچوب بر اساس استانداردهای کنترل دسترسی و اینترنت فعلی است؛
- هیچ پیام اضافی با دستگاه در مقایسه با استقرار فعلی بدون کنترل دسترسی رد و بدل نمیشود؛
- زمان اجرای یک دستگاه محدود منطقی می باشد.

چالش این کار انطباق رویکردهای استاندارد از حوزه های دیگر به محدودیتهای منابع اعمال شده توسط تنظیمات اینترنت اشیاء است.

ادامه مقاله به شرح زیر سازماندهی شده است. در بخش دوم، درمورد کارهای مرتبط در این حوزه بحث کرده و اطلاعات پس زمینه مورد نیاز برای درک این چارچوب را ارائه میدهیم. نیازهای خود را برای یک چارچوب اعتبارسنجی اینترنت اشیا در بخش سوم مطرح میکنیم. بخش چهارم چارچوب کلی در رابطه با نیازمندی ها توصیف شده، و بخش پنجم احراز هویت کاندید و پروتکلهای ایجاد کلید مورد بحث قرار خواهد گرفت. رویه های مجوز ضروری در بخش ششم و نهاد اصلی چارچوب یعنی موتور اعتبار سنجی در بخش هفتم شرح داده شده است. ما نتایج پیاده سازی را در بخش هشتم مورد بحث قرار داده و امنیت این چارچوب را در بخش نهم بررسی میکنیم. در نهایت، بخش دهم خلاصه ای از مقاله را ارائه داده و به بررسی کارهای احتمالی آینده در این حوزه می پردازد.

2. کارهای مرتبط

پروژه معماری اینترنت اشیاء اتحادیه اروپا در حال کار بر روی یک چارچوب کلی برای اینترنت اشیا از جمله امنیت آن است. به عنوان بخشی از پروژه، این کنسرسیوم مفهومی برای حفظ حریم خصوصی و امنیت برای خدمات اینترنت اشیا منتشر کرده است [1]. این مفهوم شامل استفاده از زبان نشانه گذاری کنترل دسترسی توسعه پذیر (XACML) [2] و زبان نشانه گذاری اعلان امنیت (SAML) [3] برای اینترنت اشیا است اما اقتباسات یا تغییرات این استانداردها را مورد بحث قرار نمیدهد که برای عملکرد موثر در محیط های محدود ضروری اند.

Naedele [4] یک پروتکل مبتنی بر کلید عمومی برای دسترسی و ارتباطات امن را با استفاده از یک موتور اعتبارسنجی بک اند و قابلیت های امضاشده پیشنهاد می کند. دستگاه پس از تایید اعتبار توانایی ها، یک جلسه محافظت شده با یک کاربر آغاز میکند که بعدا برای برقراری ارتباط استفاده می شود. با این حال، این پروتکل نیاز به چند تبادل پیام به منظور ایجاد یک جلسه امن داشته و فاقد گزینه شرایط محلی دستگاه است و با استانداردهای مربوطه سازگار نیست.

Resch و همکاران روشهای سبک وزن برای ایجاد امنیت زیرساخت های جغرافیایی با واحدای قدرت کم را در [5] مورد بررسی قرار دادند. این سناریو که بسیار شبیه به آنچه ما در نظرداریم است و نتایج آن نیز به سناریوی

ما اعمال می شود. نویسندگان همچنین یک چارچوب امنیتی نوین را پیشنهاد میکنند. در مقابل چارچوب پیشنهادی ما، این چارچوب براساس یک تابع پروکسی امنیتی در شبکه ایجاد شده است. مساله امنیت پایان به پایان برای سرویس را از بین میبرد که یکی از نیازهای اساسی ما خواهد بود (بخش 3 را ببینید).

Zhang و همکاران [6] یک طرح کنترل دسترسی حریم خصوصی توزیع و حفاظت شده برای شبکه های حسگر توصیف میکنند. پروتکل آنها کاربران را به خرید توکن هایی از صاحب دستگاه به منظور دسترسی به داده ها از دستگاه وادار میکند. تمرکز اصلی این کار در حفظ حریم خصوصی کاربر به سمت دستگاه و جلوگیری از استفاده مجدد از توکن تکیه دارد. این پروتکل اجرای کنترل دسترسی finegrained را بر روی دستگاه ها، و همچنین شرایط محلی آزمایش نمیکند.

به طور خلاصه می توان گفت که مشکل اعتبارسنجی در اینترنت اشیاء بطور قطعی هنوز حل نشده است. روش های فعلی بر روی تعدادی از مشکلات بسیار خاص تمرکز کرده اند، در حالی که رویکرد ما طراحی یک چارچوب اعتبارسنجی عمومی بر اساس استانداردهای موجود و یا در حال ظهور است. نوآوری رویکرد ما این است که ما پروفایل ها و توافق هایی با این استانداردها برای بهینه سازی کاربرد دستگاه های محدود طراحی کرده ایم.

3. الزامات چارچوب اعتبارسنجی

همانطور که قبلا توضیح داده شد، ما یک محیط از دستگاه های محدود و نهادهای مختلف با دسترسی به این دستگاه ها را مورد هدف قرار داده ایم. برای این محیط مجموعه ای از نیازمندی های امنیتی و اجرایی یک چارچوب اعتبارسنجی عمومی را لیست میکنیم. Naedele [4] نیز موارد نیاز را بصورت مشابه لیست کرده است، بنابراین ما خودمان را محدود به شرایط اضافی حمایت از اعتبارسنجی ریز دانه و انعطاف پذیر نموده ایم:

- R1: این چارچوب باید از

الف: قوانین دسترسی متفاوت برای درخواستهای مختلف مشتریان،

ب : کنترل دسترسی در منابع RESTful گرانولی ،

ج: سیاستهای مبتنی بر شرایط محلی (به عنوان مثال، وضعیت ، زمان، موقعیت دستگاه) پشتیبانی کند.

• R2: تمام مکانیزم های امنیتی معرفی شده باید طوری طراحی شوند که سربار محاسباتی و به خصوص ارتباطی را تا جایی که ممکن است کم کنند.

• R3: چارچوب اعتبارسنجی باید از دسترسی ایمن به اطلاعات مرتبط با کنترل دسترسی پشتیبانی کند.

• R4: راه حل های کنترل دسترسی باید وابسته به حداقل یک تابع دیگر باشد.

• R5: این راه حل باید حفاظت پایان به پایان (یکپارچگی و محرمانه) بخش های مربوط به پیامهای پروتکل، و همچنین حفاظت پاسخ را فراهم کند.

توجه داشته باشید که به منظور قابل اجرا بودن، چارچوب اعتبارسنجی پیشنهادی نباید وابسته به یک مکانیزم احراز هویت خاص، مدیریت کلید یا پروتکل انتقال امن باشد. این مکانیزم های امنیتی نیز باید با شرایط مشابه مطابقت داشته باشند. این مساله خارج از حوزه این پژوهش است، اما در طراحی اثبات مفهوم ما نهفته است.

4. چارچوب اعتبارسنجی

به منظور تحقق الزامات موردنیاز برای کنترل دسترسی ریز دانه ما از استاندارد کنترل دسترسی XACML [2] استفاده میکنیم، چراکه این استاندارد برتر در این حوزه است، و در صنعت تا حدی[1] استفاده می شود. با XACML می توانیم هر دو موارد نیاز R1.a و R1.b را پوشش دهیم.

ارزیابی سیاست های XACML برای دستگاه های محدود بسیار سنگین است، بنابراین ما اکثر فرایندهای تصمیم گیری اعتبارسنجی را اجرا کرده (R2)، و بطور کلی دستگاه اعتبار سنجی را انجام میدهد (R5).

به منظور مقابله با شرایط محلی موثر بر تصمیم گیری کنترل دسترسی (R1.c)، یا اطلاعات در مورد شرایط محلی باید به یک نقطه تصمیم گیری سیاست خارجی منتقل شوند و یا برخی از تصمیم گیری های کنترل دسترسی در داخل دستگاه محدود گرفته شوند. حالت دوم به چند دلیل ارجح است: انتقال اطلاعات در مورد شرایط محلی برای هر سیاست تصمیم گیری با مساله تاخیر روبروست و هزینه های انتقال را به دستگاه اعمال میکند، علاوه بر این، شرایط محلی ممکن است در زمان اجرا تغییر کند. همچنین می توانیم شرایط محلی را به

[1] http://www.axiomatics.com/customers.html

عنوان وظایف XACML بیان کنیم، به عنوان مثال محدودیت های تحت یک تصمیم اعتبارسنجی خارجی معتبر هستند.

به منظور انتقال تصمیمات اعتبارسنجی از نقطه تصمیم گیری های خارجی به دستگاه، ما تصمیم به استفاده از اعلان ها گرفتیم که به صورت دیجیتال اشیاء داده حاوی اطلاعات اعلان را امضا کرده اند و به ویژه از اعلان تصمیم اعتبارسنجی SAML [7] به عنوان یک الگو استفاده میکنیم. به عنوان جایگزین اعلان ها، میتواند استفاده از توکن های دسترسی OAuth به عنوان نقطه شروع باشند که نتیجه نهایی آنها مشابه بوده است، اما ما SAML را انتخاب میکنیم چراکه به خوبی با XACML ادغام میگردد.

بنابراین به سه نهاد در این چارچوب نیاز داریم: یک دستگاه (D) میزبان منابع، یک کاربر (U) مایل به دسترسی به یک منبع و یک موتور اعتبارسنجی (AE) واقع در بک اند، که ارزیابی سیاست اجرا و مسائل اعلان های اعتبارسنجی را برای دسترسی منابع به کاربر انجام میدهد. کاربر این اعلانات را همراه با درخواست خود به دستگاه می فرستد. AE به نمایندگی از صاحب دستگاه که سیاستهای دسترسی به منابع را پیکربندی کرده است عمل میکند.

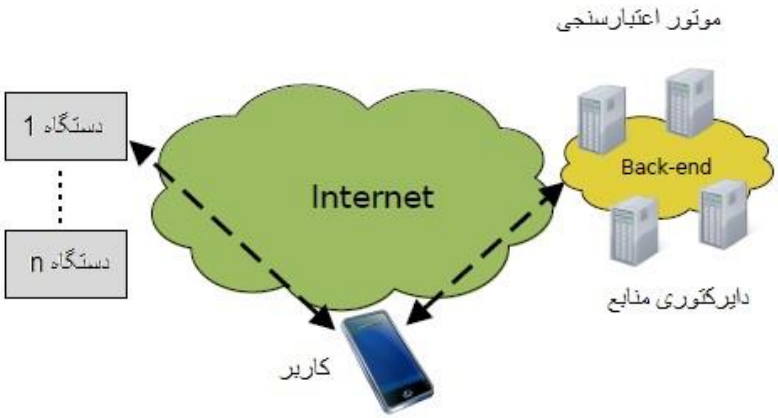
مستقل از مکانیزم اعتبارسنجی، ما همچنین به یک نهاد چهارم نیاز داریم که کشف منابع را تسهیل می سازد ، یک فهرست منابع با حفظ توصیف آنها. طراحی پیشنهادی ما استفاده از دایرکتوری را جهت مدیریت داده های امنیتی مربوط به دستگاه ها را گسترش میدهد (به عنوان مثال کلید عمومی دستگاه ، قابلیت پردازش شرایط محلی). لازم به ذکر است که به دلیل حفظ حریم خصوصی، توصیف منابع نیز ممکن است مشروط به کنترل دسترسی باشد (R3 را ببینید)، و نباید از طریق یک کانال محافظت نشده منتقل شود. اعمال چارچوب کنترل دسترسی ما به این داده ها ساده است، اما بیش از این در این مقاله مورد بحث قرار نمیگیرد.

معماری به دست آمده در شکل 1 نشان داده شده است.

با توجه به این معماری، چارچوب اعتبارسنجی نیاز به حداقل مجموعه ای از توابع دارد (R4 را درنظر بگیرید):

• AE باید قادر به اتصال کاربر به اعلان باشد. اگر تصمیم اعتبارسنجی به هویت کاربر بستگی داشته باشد، AE همچنین نیاز به تأیید هویت کاربر خواهد داشت. در مواردی که هویت کاربر مشخص نیست (به عنوان مثال یک سرویس خریداری شده) از نام مستعار می توان استفاده کرد. اتصال را می توان با کلید عمومی یا نام مستعار

کاربر در اعلان به دست آورد. نام مستعار را می توان با استفاده از طرح توصیف شده در بخش 5 تایید کرد.



شکل. 1: معماری اعتبارسنجی

• دستگاه باید بتواند تایید کند که یک اعلان معتبر بوده و از یک منبع قابل اعتماد است. برای رسیدن به این امر، AE نیاز به ثبت پیام با استفاده از یک کلید است که توسط دستگاه شناخته شده و مورد اعتماد آن است.

• دستگاه باید قادر به اتصال کاربر به اعلان باشد. این را می توان با احراز هویت صریح یا ضمنی کاربر (یا نام مستعار مورد استفاده) به دست آورد.

برای تطابق با R2 پروتکل مورد استفاده برای اجرای این توابع باید از حداقل تبادل پیام با دستگاه استفاده کند، بطور ایده آل نه بیش از اینکه اگر دستگاه بدون مکانیزم اعتبارسنجی مورد دسترسی قرار بگیرد. همانگونه که پروتکل انتقالی که بر روی پیش نویس پروتکل کاربرد محدود IETF نوشته ایم (COAP) اطلاعات امنیتی به پیامهای COAP در هنگام نیاز اضافه میشوند. COAP به طور خاص برای دستگاه های محدود طراحی شده و یک سربار بسیار کم در مقایسه با مثلا HTTP نشان میدهد، با این حال چارچوب پیشنهادی مختص COAP نیست و با دیگر پروتکل های لایه کاربرد کار میکند.

با چارچوب توصیف شده فوق می توان توابع مطابق با تمام نیازهای خود و حتی نیازمندی های Naedele را پیاده سازی کرد [4].

5. ایجاد کلید

نیازمندی R5 یک روش ایجاد کلید فرض میکند، که در آن کلید تامین شده و به نوبه خود توسط یک روش احراز هویت بوجود می آید. چارچوب اعتبارسنجی ما نه نیاز به یک پروتکل احراز هویت خاص دارد و نه روش توافقی کلید، اما با این حال باید چگونگی تشکیل کلیدها را درنظر بگیریم چرا که روی ظرفیت باقیمانده دستگاه برای کارهای اعتبارسنجی مربوط تاثیر میگذارد. ما خود را به دو کاندید اصلی در اینجا محدود کرده ایم.

یکی از گزینه های مناسب برای COAP , DTLSبر اساس کلیدهای عمومی و یا کلیدهای از پیش مشترک است [10]، که در این صورت پروتکل ضبط DTLS رمزگذاری، جامعیت و حفاظت پخش پیام های COAP را فراهم می کند. برای دستگاه های بسیار محدود، با این حال، DTLS ممکن است زمان راه اندازی قابل توجهی را تحمیل کند.

به عنوان اثبات مفهوم، چارچوب در یک رویکرد مبتنی بر امنیت شی مدل شده است. این رویکرد از کلید متقارن برای حفاظت اشیا استفاده میکند اما با هر دو کلید متقارن و نامتقارن کار میکند: فرض اول این است که دستگاه و موتور اعتبارسنجی کلیدهای عمومی یکدیگر را ایجاد کرده اند. استفاده از این کلیدهای عمومی استاتیک در یک محاسبه Diffie-Hellman امکان پذیر است که یک کلید مشترک متقارن سری kAD (C(0e; 2s) را با طرح [11] استخراج میکند. همچنین با درنظرگرفتن یک کلید عمومی تایید شده از کاربر در اعلان (که توسط موتور اعتبارسنجی در درخواست اعلان تعیین میشود) و یک nonce در ظرفیت بار، دستگاه و کاربر می توانند محاسبات آنالوگ انجام داده و یک کلید متقارن KUD استخراج کنند.

حال فرض کنید که دستگاه و موتور اعتبارسنجی کلیدهای متقارن مشترک ایجاد کنند. با درنظر گرفتن یک نام مستعار کاربری منحصر به فرد به جای کلید عمومی در این اعلان، موتور اعتبارسنجی و دستگاه می تواند از یک تابع اشتقاق کلید یک طرفه مناسب برای استخراج یک کلید KUD متقارن استفاده کنند، که همچنین در پاسخ به درخواست اعلان به کاربر ارائه میشود. همچنین در این مورد درنظر گرفتن یک nonce در یک شئ و اشتقاق کلید برای جلوگیری از استفاده بیش از حد از کلیدها معقول است.

از این رو با توجه به هر نوع استقرار کلید بین دستگاه و AE ما می توانیم بدون از دست دادن کلیت فرض کنیم که کلیدهای متقارن به اشتراک گذاشته شده KAD و KUD با AE و U، به ترتیب بعد از دریافت این اعلان

در دستگاه موجود می باشند. این کلیدهای به اشتراک گذاشته پایه ای برای تامین امنیت اشیاء داده در حال عبور بین AE و D (اعلانات)، و U و D (ظرفیت بار) هستند.

لازم به ذکر است که روشهای ترکیبی نیز وجود دارد، به عنوان مثال، DTLS طولانی بین دستگاه و AE برای ایجاد یک کلید مشترک استفاده میشود که می تواند برای استخراج کلید KUD برای تأمین امنیت اشیاء درحال انتقال بین کاربر و دستگاه مورد استفاده قرار میگیرد.

6. روش اعتبارسنجی

به عنوان یک نتیجه از چارچوب مشخص شده در بخش 5، به مجموعه ای از روش ها و پروتکل ها در انجام وظایف زیر نیاز داریم:

A. ثبت دستگاه های جدید توسط صاحبان دستگاه و داده های امنیتی مربوط به آنها.

B. کاربرانی که به دنبال یک دستگاه بوده و درخواست یک اعلان اعتبارسنجی برای آن دارند.

C. کاربرانی که به یک دستگاه با استفاده از یک اعلان اعتبارسنجی قبلا به دست آمده دسترسی دارند.

به منظور تطابق با نیازمندی R2 ، پروتکل ها را به طوری طراحی کرده ایم که به تبادل پیام های اضافی نسبت به مبادلات COAP محافظت نشده نیازی نداشته باشند.

A. ثبت دستگاه های جدید

در این عملیات، فرض میکنیم یک دایرکتوری منابع مانند فهرست منابع IETF وجود دارد که از روش های آغاز ثبت توصیف منابع به دایرکتوری دستگاه پشتیبانی میکند. فرض می کنیم که اطلاعات مربوط به امنیت برای دستگاهی مانند کلیدی عمومی آن، AE که به آن اعتماد دارد، صاحب آن و تعهداتی که می تواند انجام دهد، ممکن است به عنوان متا داده دستگاه در دایرکتوری ثبت شده و می تواند توسط نهادهای مربوطه پرس وجو شود. انتشار این متا داده می تواند از همان روش انتشار منابع دستگاه پیروی کند.

B. دریافت اعلان اعتبار

به منظور دسترسی به یک منبع در یک دستگاه، کاربر نه تنها نیاز به پیدا کردن URI آن منبع دارد، بلکه باید یک اعلان اعتبار و یک کلید رمزنگاری برای استفاده در پروتکل های امنیتی با دستگاه بدست آورد. URI منبع و پارامترهای امنیتی مربوط به دستگاه را می توان از فهرست منابع بازیابی نمود. در این میان آدرس AE مورد اعتماد دستگاه است.

کاربر یک اعلان برای دسترسی به یک منبع خاص از این AE درخواست میکند، که بطور داخلی پروتکل درخواست پاسخ XACML را برای پیداکردن دسترسی کاربر اجرا می شود (بخش هفتم را ببینید). اگر چنین است، AE یک اعلان و یک کلید دستگاه به کاربر برمی گرداند.

بسته به اینکه کلید نامتقارن یا متقارن استفاده شود، این اعلان شامل یک کلید عمومی و یا یک نام مستعار منحصر به فرد از کاربر است. در مورد اول، کلید دستگاه کلید عمومی دستگاه است. در مورد دوم، کلید دستگاه از کلید مخفی KUD مشتق شده است (بخش پنجم). این اعلان با استفاده از کلید نامتقارن یا متقارن AE امضا[۲] شده است.

پروتکل، مکانیزم احراز هویت و انتقال امن بین کاربر و AE خارج از محدوده این مقاله است. فرض کنید که کاربر و AE منبع محدود نیست، استانداردهای اینترنت معمول مانند HTTP و TLS نیز می تواند اعمال شود.

C. دسترسی به یک دستگاه

به منظور دسترسی به منابع روی دستگاه، کاربر یک درخواست COAP شامل اعلان به دستگاه ارسال می کند، که با یک مجموعه پروتکل / رمزنگاری پشتیبانی شده توسط دستگاه ایمن شده است. COAP از استفاده از اطلاعات درخواست اختیاری که به عنوان یک گزینه COAP پراکنده بین هدر و ظرفیت بار منتقل میشود، پشتیبانی میکند. ما یک گزینه اعلان در COAP معرفی می کنیم. علاوه بر این، در رویکرد امنیت شی، ظرفیتهای بار COAP معادل اشیاء امن بر اساس کلید دستگاه را جایگزین میکنیم.

[2] اصطلاح امضا برای تایید کدهای پیام نیز استفاده می شود

دستگاه این اعلان را تایید میکند، و حقوق دسترسی مجاز در این اعلان را با درخواست دسترسی واقعی مطابقت داده و شرایط محلی (در صورت وجود) مشخص شده در این اعلان را تایید میکند.

اگر تمام تاییدیه ها موفق باشند، درخواست با پردازش و پاسخ متعاقب انجام می شود. حفاظت پاسخ با دادن یک زمان اعتبارسنجی کوتاه از پیش تعریف شده به اعلانات، و ذخیره لیستی از شناسه های اعلانات اخیرا استفاده شده بر روی دستگاه فراهم میشود.

در حالی که DTLS رمزگذاری همراه و حفاظت جامعیت ظرفیت بار و هدر را ارائه می کند، رویکرد امنیتی اشیاء اجازه یک تبادل بین محافظت در برابر عملکرد خواهد داد. بسته به مدل اعتماد، اعلان و ظرفیت بار ممکن است به رمزگذاری نیاز داشته باشد زیرا استراق سمع اطلاعات در مورد درخواست کاربر را آشکار میکند، که ممکن است نسبت به حریم خصوصی حساس باشند. بسته بندی ظرفیت های بار به عنوان اشیاء امن، حفاظت متفاوتی از محتوا بر اساس حساسیت آن اجازه می دهد.

برای مثال، در یک درخواست COAP GET، اعلان می تواند تنها بطور یکپارچه محافظت می شود، در حالی که ظرفیت بار پاسخ را می توان بصورت رمزگذاری و یکپارچه محافظت کرد. در یک CoAP PUT/POST اعلان و درخواست ظرفیت بار بطور یکپارچه محافظت شده و این پاسخ محافظت نشده خواهد بود.

پارامترهای امنیتی منتشر شده توسط دستگاه باید مشخص کند که کدام حالت حفاظتی مورد استفاده قرار گیرد و کدام شناسه رمزنگاری ترجیحا باید استاندارد شود.

7. موتور اعتبارسنجی

موتور اعتبارسنجی شامل دو جزء است: سیستم کنترل دسترسی و سیستم صدور اعلان.

سیستم کنترل دسترسی تصمیمات کنترل دسترسی مبتنی بر سیاست با استفاده از XACML تولید میکند. نحوه ایجاد سیاست و مدیریت آن خارج از حوزه این مقاله است.

زمانی که درخواست یک کاربر توسط سیستم کنترل دسترسی پذیرفته شود، سیستم صدور اعلان تصمیم اعتبارسنجی را به عنوان یک اعلان رمزگذاری میکند.

این امکان وجود دارد که دسترسی پذیرفته شده توسط این اعلان به پارامترهای شناخته شده دستگاه بستگی داشته باشد، که در این صورت دستگاه آنها را ارزیابی کرده و دسترسی را رد یا قبول میکند. به این معنی که حداقل برخی از دستگاه ها اعمالی بیشتر از تصمیمات خالص کنترل دسترسی اجرا میکنند.

برای قادر کردن دستگاه به اجرای تصمیمات اعتبارسنجی، اعلان نیاز به ارائه اطلاعات زیر دارد:

• کدام منبع تصمیم گیری میکند.

• کدام عمل (GET، PUT، POST، DELETE) کند برای تصمیم اعمال می شود.

• موضوع درخواست تصمیم چیست و چگونه می تواند تصدیق شود (در صورت لزوم).

• موتور اعلان که این اعلان را صادر کرده است کدامست (این اطلاعات ممکن است بطور ضمنی از امضای اعلان استخراج شوند).

• این اعلان تحت چه شرایطی اعتبار دارد (تاریخ انقضا، حفاظت پاسخ، پارامترهای ارزیابی شده توسط دستگاه در زمان دسترسی).

از آنجا که سینتکس کامل پاسخهای XACML و اعلانات SAML شامل ویژگی های زیادی است، ما زیر مجموعه ای از هر دو استاندارد به منظور ساده سازی پردازش بر روی دستگاه تعریف کرده ایم. علاوه بر این، ارائه XML این زیر مجموعه برای انتقال کارآمد روی کانالهای محدود بیش از حد طولانی است، بنابراین ما یک نماد مبتنی بر JSON فشرده برای SAML و زیر مجموعه XACML تعریف کرده ایم. این رویکرد اندازه اعلان را تقریبا با عاملی از ده کاهش می دهد.

اعلان نشان داده شده در مثال زیر با اندازه 208 بایت بدون چاپ زیبا دارد. XML مربوطه اعلان به اندازه 2281 بایت خواهد بود.

```
01 {
02   "ID": "ID_ffda55f9...097bdd21e6",
03   "II": "2013-02-15T10:02:52Z",
04   "IS": "AAA-Server",
05   "SK": "BvDgLAXSHe...0RLhfwS1fue",
06   "ST": {
07     "OB":{
08       "NB":"09:00:00Z",
09       "NA":"17:00:00Z"
10     },
11     "ACT": "GET",
12     "RES": "coap://node346/tempSensor"
13   }
14 }
```

ID شناسه اعلان ، II نمونه موضوع در فرمت UTC ، IS شناسه صادر کننده اعلان و SK نشان دهنده موضوع اعلان با استفاده از یک کلید عمومی برای تایید موضوع است.

عبارت تصمیم اعتبارسنجی توسط ST نشان داده شده است، شامل عبارت مختصر XACML تعهد OB است که شرایط محلی را نشان میدهد که بر روی دستگاه تایید شده است. در این مورد ما یک زمان نه قبل از (NB) و نه بعد از (NA) که اجازه دسترسی را محدود میکند داریم.

المان ACT عمل است و منبع هدف URI RES مجاز توسط اعلان می باشد. این پارامترها نشان دهنده درخواست XACML هستند.

توجه داشته باشید که پاسخ XACML به یک پاسخ PERMIT دلالت دارد. موتور اعتبارسنجی برای تصمیم گیری اعلانهایی بجزPERMIT صادر نمیکند. علاوه بر این بخش موضوع درخواست XACML حذف شده است از آنجا که موتور اعتبارسنجی که به عنصر SK اعلان مربوط است اجرا میشود.

دستگاه باید بداند که چگونه تعهدات را پردازش کند، در غیر این صورت باید اعلان را رد کند. بخش ششم نحوه انتشار انواع تعهداتی که یک دستگاه که می تواند پردازش کند را توضیح می دهد.

8. پیاده سازی

بخشی از دستگاه در چارچوب ما با استفاده از رویکرد مبتنی بر امنیت اشیا و کلیدهای متقارن (در بخش5) بر روی یک پلت فرم نمونه اجرا شد: Arduino Mega board3 2560. این برد دارای یک پردازنده 16

مگاهرتز، 256 کیلوبایت حافظه فلش، 8 کیلو بایت SRAM ، و 4 کیلوبایت EEPROM است. ما این برد را به منظور تست رویکرد خود در پایان طیف عملکردی برای دستگاه های محدود موردهدف انتخاب کردیم.

این برد در C با استفاده از یک اجرای سفارشی از پشته پروتکل COAP ، کتابخانه Cryptosuite برای HMAC-SHA256 و یک بهینه سازی 8 بیتی AES اجرای توسط Brian Gladman برنامه نویسی شده است.

پردازش پیامهای COAP بر روی دستگاه، از جمله دستکاری اعتبارسنجی ما، نیاز به حدود 7.3 کیلو بایت حافظه استاتیک دارد (از جمله Arduino داخلی مانند UDP، اترنت، کتابخانه SPI و غیره)، که به ما مکان های نزدیک به حد بالایی از این برد که می تواند انجام دهد را خواهد داد.

از وقت گیرترین عملیات مورد نیاز ، جای تعجب نیست که رمزنگاری ، رمز گشایی، حفاظت یکپارچه، و بررسی یکپارچگی می باشند. ثابت شده که عملیات دیگر مانند تطبیق اعلان به عمل درخواست شده تنها زمان ناچیزی مصرف میکنند.

ما تصمیم به استفاده از رمزگذاری IETF JSON وب کردیم (JWE) [13]، که یک استاندارد امنیت اشیاء در حال ظهور برای بسته بندی اعلانات و ظرفیت بار است. لازم به ذکر است که این بسته بندی به شدت اندازه ظرفیت بار را گسترش می دهد. به عنوان مثال خواندن یک سنسور معمولی می تواند یک عدد صحیح 4 بایتی باشد. در صورتی کهبا رمزگذاری AES و یک کد تأیید هویت پیام HMAC محافظت شود، 128 بایت متن رمز شده به دلیل بسته بندی اندازه بلوک و 160 بایت دیگر برای MAC خواهیم داشت.

جدول 1 آمار و ارقام عملکرد نتیجه را نشان می دهد.

تایید یکپارچگی اعلان / درخواست POST	58 ms / 100 ms
رمزگشایی اعلان / درخواستPOST	231 ms
رمزگذاری پاسخ GET	192 ms
حفاظت یکپارچگی پاسخ GET	101 ms

جدول 1 زمان اجرای فرایند رمزنگاری

زمانهای پردازش با اندازه گیری زمان رفت و برگشت یک پیغام POST حفاظت شده و یک پیام GET محافظت شده در کلاینت COAP تایید میشود، که برابر با مجموع ارقام متناظر در جدول به علاوه یک زمان ثابت مربوط به زمان رفت و برگشت پیام بدون محافظت است.

این تستها از یک تراشه بدون هیچ کمک پردازنده رمزگذاری استفاده کرده اند. با استفاده از چنین سخت افزار تخصصی می توان مصرف حافظه و مصرف باتری را کاهش داد و کارایی را بهبود بخشید.

9. ارزیابی امنیت

در چارچوب حاضر، هدف ما محافظت از موارد زیر است: داده های روی دستگاه ها، خود دستگاه ها ، و خدمات ارائه شده توسط دستگاه ها.

معیار ما برای حفظ این موارد ، رعایت محدودیت های finegraine در دسترسی به دستگاه ها است (به عنوان یک مخالفی با یک رویکرد همه یا هیچ ، که فقط نیاز به احراز هویت دارند). با توجه به راه اندازی چارچوب پیشنهادی، ما نیز به حفاظت از تصمیمات اعتبارسنجی، سیاست های اعتبارسنجی، و ویژگی های مربوط به این تصمیمات نیازمندیم.

لازم به ذکر است که تنها حفاظت از تصمیمات اعتبارسنجی نیاز به تایید بر روی دستگاه دارد، هرچیز دیگری بر روی ماشین های قوی تر بک اند اجرا می شود.

موتور اعتبارسنجی یک شخص ثالث مورد اعتماد از نقطه نظر صاحب دستگاه است، که اگر به خطر بیافتد می تواند به عنوان مثال اعلانهای اشخاص غیر مجاز را صادر کرده و یا از یک کلید KUD مشتق شده برای رمزگشایی یک پاسخ GET استراق سمع استفاده نماید.

تنظیمات امنیتی پایان به پایان دو طرفه است. از آنجا که تمام داده ها در دستگاه تایید شده و حفاظت شده اند، هیچ هدف حمله واسطه ای برای شکستن اعتماد و یکپارچگی وجود نخواهد داشت. بلکه از آنجا که دستگاه در اصل برای دسترسی اختیاری کاربران است، مکانیزم های حفاظت اضافه بار ممکن است مورد نیاز باشند، به عنوان مثال قابلیت فایروال خارجی محدود به تعداد درخواستهای همزمان و / یا تایید اعلانها قبل از انتقال (در صورت امکان).

یک روش جایگزین استفاده از یک دروازه است که دسترسی کامل و مستقیم به دستگاه هایی دارد که آنها را مدیریت کرده و درخواست های دسترسی را بر اساس سیاست های کنترل دسترسی خود فیلتر میکند. چنین رویکردی این مزیت را دارد که تمام اقدامات اعتبارسنجی به یک نهاد بدون محدودیت منبع موجود بر روی دستگاه ها منتقل میشود. با این حال اشکال این است که نمی توانیم حفاظت پایان به پایانی از پیام های پروتکل نگه داریم، چون دروازه باید قادر به خواندن آنها باشد. بنابراین درخواستهای حیاتی حریم خصوصی نمی تواند محافظت شود و کاربر باید به دروازه بی اعتماد باشد. علاوه بر این، این روش در یک سناریوی با دستگاه های فقط به صورت محلی در دسترس در مکان های مجزا قابل اجرا نیست.

10. نتیجه گیری و کارهای آتی

ما یک چارچوب اعتبارسنجی عمومی برای دستگاههای اینترنت اشیا ساخته شده براساس استانداردهای اینترنت و کنترل های دسترسی موجود با پشتیبانی از کنترل دسترسی ریز دانه و انعطاف پذیر برای دستگاه های محدود ارائه کردیم.

مولفه های کلیدی این چارچوب ، موتور اعتبارسنجی، پروفایل اعلان تعریف شده به عنوان زیر مجموعه ای از SAML و XACML و نمایش فشرده در یک نماد JSON است. با اهمیت ویژه ای ما از قوانین XACML برای فعال کردن هر نوع تصمیم گیری محلی در دستگاه استفاده کرده ایم. اجزای پشتیبانی، تعمیم انتشار فهرست منابع قابلیت های دستگاه برای تصمیم های محلی و اجرایی هستند، و روش های مدیریت کلید برای برقراری امنیت بین دستگاه و AE /کاربر مورد استفاده قرار میگیرند.

بخش های حیاتی عملکرد این چارچوب با استفاده از یک رویکرد مبتنی بر امنیت اشیاء بر روی یک دستگاه نمونه اجرا و تست شده شده است و نتیجه نشان داده است که روش های اعتبارسنجی می تواند در یک چارچوب زمانی معقول در کلاس های خاصی از دستگاه های محدود اجرا شوند. ارزیابی امنیتی تبادلات و مفروضاتی نشان میدهد که برای این چارچوب ساخته میشوند و تعیین میکند که این چارچوب چه تضمین های امنیتی فراهم می کند.

استفاده از JWE به عنوان فرمت بسته بندی شی امن برای اعلان مناسب است، اما برای ظرفیتای بار چند بایت که در COAP معمول است، نا مطلوب می باشد. هر دو هدر JWE و ظرفیت بار رمزنگاری شده می تواند برای این نوع از استقرار فشرده شوند. کارهای آینده بالقوه عبارتند از کاوش و استانداردسازی استفاده از جریانهای رمز و MAC برای JWE . موضوعات دیگر برای استاندارد سازی پروفایل اعلان SAMLو XACML و ثبت دستگاه از متاداده مربوط به امنیت با استفاده از فهرست منابع است.

سپاسگذاری

ما می خواهیم از Alexander Maximovاز مرکز تحقیقات اریکسون بخاطر بهینه سازی کدAES 8 بیتی او تشکر نماییم.

REFERENCES

[1] A. Serbanati, A. S. Segura, A. Oliverau, Y. B. Saied, N. Gruschka, D. Gessner, and F. Gomez-Marmol, "Internet of Things Architecture, Concept and Solutions for Privacy and Security in the Resolution Infrastructure," EU project IoT-A, Project report D4.2, February 2012, http://www.iot-a.eu/public/public-documents.

[2] S. Godik, and T. Moses (eds.), "eXtensible Access Control Markup Language (XACML)," Organisation for the Advancement of Structured Information Standards (OASIS), Standard Version 2.0, February 2005. [Online]. Available: http://www.oasis-open.org/committees/xacml

[3] S. Cantor, J. Kemp, R. Philpott, and E. Maler (eds.), "Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML)," Organisation for the Advancement of Structured Information Standards (OASIS), Standard Version 2.0, March 2005. [Online]. Available: http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

[4] M. Naedele, "An Access Control Protocol for Embedded Devices," in *Proceedings of the fourth IEEE Conference on Industrial Informatics, INDIN*. Singapore: IEEE, August 2006, pp. 565–596.

[5] B. Resch, B. Shulz, M. Mittlboeck, and T. Heistracher, "Pervasive geo-security a lightweight triple-A approach to securing distributed geo-service infrastructures," *International Journal of Digital Earth*, vol. 5, no. 4, pp. 1–18, 2012.

[6] R. Zhang, Y. Zhang, and K. Ren, "Distributed Privacy-Preserving Access Control in Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 8, pp. 1427–1438, 2012.

[7] E. Rissanen, and H. Lockhart (eds.), "SAML 2.0 Profile of XACML Version 2.0," Organization for the Advancement of Structured Information Standards (OASIS), Committee Specification, August 2010, http://www.oasis-open.org/committees/xacml.