پژوهش در مورد مکانیزم امنیتی برای ارتباط داخلی بین پروفیباس و اینترنت

چکیده

ارتباط بین شبکه پروفیباس و اینترنت می تواند به تحقق وسیله نظارت زمان-واقعی از راه دور بر فیلدباس منجر شود. این مقاله, یک تحلیل و پژوهش مفصل را در مورد امنیت شبکه بر اساس روش های ارتباط داخلی بین پروفیباس و اینترنت انجام داده است و یک مدل امنیت شبکه صنعتی پروفیباس را پیشنهاد می کند. یک گذرگاه تعبیه شده به طور خاص برای برآورده سازی الزام امنیتی در این کار پژوهشی توسعه می یابد. با ساختار فشرده و هزینه پایین, راه به سوی تحقق وسیله نظارت پروفیباس زمان-واقعی به طور ایمن توسط اینترنت هموار می شود.

عبارات شاخص- پروفیباس، گذرگاه تعبیه شده، امنیت

1. مقدمه

پروفیباس رایج ترین فیلدباس در تولید, کنترل فرآیند و اتوماسیون است. چگونگی ایجاد دسترسی شبکه فیلدباس به اینترنت و توانمندسازی اطلاعات شرکت و کنترل ارتباط داخلی شبکه به تمرکز پژوهشی فناوری شبکه صنعتی تبدیل شده است.

شبکه صنعتی به دلیل محیط و هدف خدماتی خود, از شبکه های تجاری دیگر متفاوت است. به طور کلی, شبکه صنعتی, یک سازمان است که توسط دو بخش ساخته می شود, شبکه اطلاعات و شبکه کنترل. شبکه اطلاعات برای مدیریت این سازمان استفاده می شود. شبکه کنترل, ادوات و تجهیزات تولید را با هم مرتبط می کند و کنترل و نظارت بر فرآیند را متمرکز می سازد. در این پژوهش, شبکه کنترل بر اساس پروفیباس است. به عنوان یک واحد مستقل, محرمانگی اطلاعات تجاری و جلوگیری از هجوم هکرها, برای شبکه داخلی یک سازمان حیاتی است. برای تحقق کنترل از راه دور و مدیریت فرآیند تولید, وضعیت و پارامترهای تجهیزات تولید باید به صورت زمان واقعی ارائه شوند. به بیانی دیگر, سیستم کنترل مبتنی بر پروفیباس باید توسط شبکه صنعتی و اینترنت, دردسترس قرار گیرد.

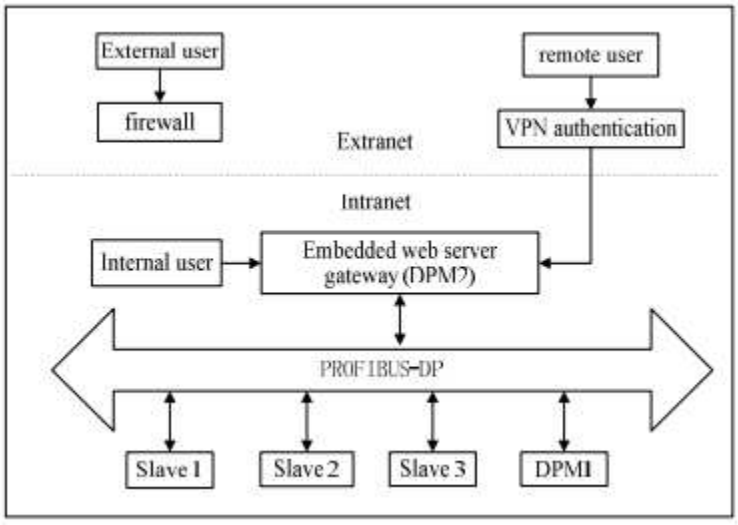
بنابراین, روش امنیت موثر و قابل اطمینان باید در ارتباط داخلی شبکه اتخاذ شود. در حال حاضر, هیچ راه حل منحصر به فردی برای حل مسائل امنیت شبکه در هنگام استفاده از گذرگاه تعبیه شده برای ارتباط به اینترنت وجود ندارد. به دلیل منابع تعبیه شده محدود, خط مشی امنیتی موجود برای PC را نمی توان به طور مستقیم مورد استفاده قرار داد. طراحی یک راهبرد امنیتی فشرده مطابق با حالت کاربرد عملی برای پروفیباس ضروری است. در این پژوهش, یک روش مبتنی بر گذرگاه وب تعبیه شده برای تحقق ارتباط داخلی بین شبکه پروفیباس-DP و اینترنت پیشنهاد می شود و برخی از روش های امنیتی فشرده برای ارائه تضمین امنیتی, در زمانی که کاربرد توسط اینترنت به وسیله پروفیباس دسترسی دارد, پیشنهاد می شوند.

II. روش دسترسی پروفیباس به اینترنت

ساختار پروتکل DP- پروفیباس, سه مدل ساختار لایه را بر اساس ISO7498 اتخاذ می کند, از جمله, لایه فیزیکی, لایه لینک داده ها و لایه واسطه کاربر. در حالیکه TCP/IP, چهار مدل ساختار لایه را اتخاذ می کند, از جمله لایه واسطه شبکه, لایه شبکه, لایه حمل و نقل و لایه کاربرد. برای تحقق ارتباط داخلی و برقراری ارتباط بین دو نوع شبکه ناهمگون, یک روش مناسب باید برای اتصال شبکه پروفیباس با اینترنت اتخاذ شود.

در حال حاضر, چهار نوع وسیله برای ارتباط داخلی شبکه وجود دارند, از جمله تکرارکننده, پل, روتر (مسیریاب) و گذرگاه. گذرگاه که به عنوان مبدل پروتکل شبکه نیز نامیده می شود برای پیاده سازی ارتباط داخلی و برقراری ارتباط بین شبکه های ناهمگون استفاده می شود. بنابراین یک گذرگاه تعبیه شده برای تحقق ارتباط داخلی بین شبکه پروفیباس و اینترنت در این پژوهش استفاده می شود. با پیکربندی مانند این, شبکه های ناهمگون می توانند بدون تغییر ساختار اصلی شبکه با یکدیگر ارتباط برقرار کنند و حفظ سرمایه موجود, سودمند است. شکل 1, ارتباط داخلی بین DP- پروفیباس و اینترنت را با استفاده از گذرگاه نشان می دهد.

در DP- پروفیباس, تا حدود 127 وسیله, پایه یا پیرو را می توان به یک باس وصل نمود. سیستم DP- پروفیباس بین انواع وسایل زیر تمایز قائل می شود: پیرو DP, پایه DP رده 1 (DPM1) و پایه DP رده 2 (DPM2). گذرگاه سرور وب تعبیه شده به صورت یک DPM2 در شکل 1 نشان داده شده است.



شکل 1. نمایش ارتباط داخلی بین پروفیباس و اینترنت

یک سیستم DP- پروفیباس پیکربندی شده با DPM1, 3 پیرو و 1 DPM2 (گذرگاه تعبیه شده) در این پژوهش اتخاذ شده است. ساختار سیستم DP- پروفیباس با ادوات بیشتر به طور مشابه است و روش ارتباط سازگار است. مطابق با اصل آدرس دهی پروفیباس, آدرس DPM1 برابر با 1 است, آدرس DMP2 برابر با 3, آدرس های پیرو 1, پیرو 2, پیرو 3 به ترتیب 4,5,6 هستند. در اینجا, گذرگاه وب تعبیه شده عمدتاً برای انجام تبدیل پروتکل بین پروتکل پروفیباس و پروتکل TCP/IP استفاده می شود و کاربرانی را تایید می نماید که از شبکه اینترانت یا خارجی به سیستم DP- پروفیباس دسترسی دارند. در این مورد, درخواست های دسترسی شبکه باید از طریق گذرگاه عبور نماید. این مورد, حالت B/S (Browser/Server) را برای دستیابی به ویزیت کاربر از سرور تعبیه شده اتخاذ می کند.

متقاضی, درخواست دسترسی را به وسیله باس DP- پروفیباس از یک مرورگر توسط اینترنت به گذرگاه وب تعبیه شده می فرستد. بعد از تایید, گذرگاه وب تعبیه شده, درخواست را استفسار می کند یا درخواست را مطابق با متقاضی به وسیله پیرو که به عنوان شی دسترسی کاربر است کنترل می کند. وسیله پیرو, درخواست را پاسخ می دهد و داده ها را به گذرگاه منتقل می کند. در طی این فرآیند, گذرگاه, تبدیل پروتکل بین پروتکل پروفیباس و پروتکل TCP/IP, پردازش داده ها, و نیز انتشار اطلاعات تجهیزات را در شکل صفحات وب با کمک سرور وب انجام می دهد.

اولاً از نظر خط مشی امنیتی, دیوار آتش باید برای ایزوله نمودن اکسترانت و اینترانت به منظور تضمین امنیت اینترانت استفاده شود. ثانیاً, برای کاربر راه دور, آنها اجازه دارند تا دستگاه را تنها بعد از کنترل رمز عبور VPN و تایید هویت و اجازه بهره برداری نمایند. سوماً, در اینترانت, فناوری های تایید هویت و رمزگذاری داده ها برای جلوگیری از کاربران اینترانت که اطلاعات کاربران دیگر را استراق سمع می کنند, دسترسی به منابع غیرمجاز و حتی تغییر فایل های سیستم به صورت غیرقانونی استفاده می شوند. در این مقاله, خط مشی امنیتی سوم عمدتاً تحلیل و طراحی می شود.

III. تحلیل و طراحی مکانیزم امنیتی

برای اترنت صنعتی, تهدیدات امنیت, عمدتاً از دو جنبه می آید. اولین نوع تهدید عمدتاً از بازدید حمله کنندگان به منابع شبکه یا دسترسی به سیستم کنترل بدون اجازه ناشی می شود. این می تواند به از دست دادن و سوء استفاده از اطلاعات محرمانه و به خطر انداختن ایمنی سیستم منجر شود. نوع دوم از تهدید عمدتاً توسط استراق سمع حمله کنندگان و وانمود کردن اطلاعات محرمانه ناشی می شود, که این مورد عمدتاً در فرآیند ارتباط داده ها بین اینترنت و شبکه کنترل منعکس می شود.

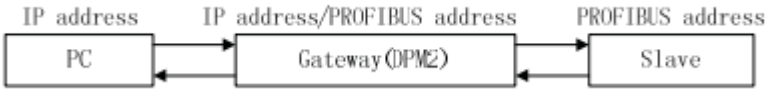
در این تحقیق, گذرگاه وب تعبیه شده به صورت سیستم عامل برقراری ارتباط اتخاذ می شود و هاب سیستم نظارت شبکه پروفیباس است. با چندین ادوات پایه و پیرو توسط DP- پروفیباس به سمت داخل ارتباط برقرار می کند و توسط LAN و Modem به سمت بیرون متصل می شود. انتقال و ارتباط داده ها بین اینترنت و DP- پروفیباس توسط گذرگاه وب تعبیه شده کنترل می شود. به دلیل ول تعبیه شده, این هاب برای کاربر در دسترسی اینترنتی به وسیله, نکته کلیدی امنیت شبکه در سیستم نظارت شبکه پروفیباس است.

مطابق با کاربرد گذرگاه وب تعبیه شده در DP- پروفیباس, مکانیزم امنیت شبکه که در این مقاله معرفی شده است, عمدتاً از سه جنبه می آید. اولاً, امنیت سیستم عامل تعبیه شده به خودی خود, مبنا است. یعنی می توان گفت که گذرگاه به خودی خود باید تضمین نماید که تبدیل پروتکل, صحیح است, این مبنای انتقال صحیح اطلاعات بین کاربرد و وسیله DP- پروفیباس است. ثانیاً, مکانیزم کنترل دسترسی باید برای ممانعت از دسترسی کاربر غیرقانونی

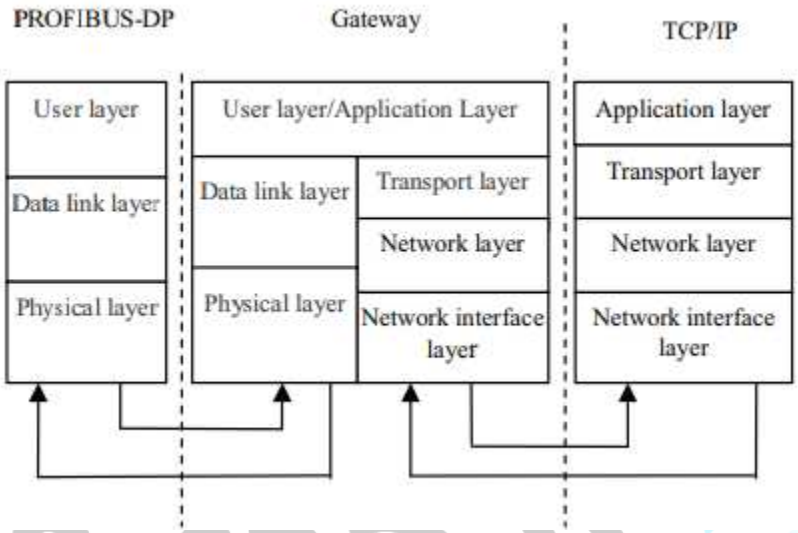
به منبع غیرمجاز اتخاذ شود. سوماً, فناوری امنیتی برای انتقال داده ها باید به منظور جلوگیری از کدگشایی اطلاعات محرمانه سیستم توسط حمله کنندگان اتخاذ شود. 2 باید اطمینان حاصل شود که داده ها, به واسطه تایید قابل اطمینان هستند و باید از حمله فعال به شبکه, مانند فضولی و وانمود کردن محافظت نمود.

A. تبدیل پروتکل

ساختار پروتکل پروفیباس و پروتکل TCP/IP, متفاوت هستند. تبدیل صحیح پروتکل, مبنای تحقق عملیات از راه دور ایمن وسیله روی DP- پروفیباس توسط اینترنت است. همانند کلاس DP پایه 2, گذرگاه طراحی شده در این مقاله, دارای آدرس های پروفیباس مستقل خود است. در عین حال, به اینترنت وصل می شوند, بنابراین دارای آدرس IP خود می باشد. دیاگرام تبدیل آدرس در شکل 2 نشان داده شده است. زمانی که کاربر روی اینترنت می خواهد به وسیله پروفیباس دسترسی داشته باشد و آن را کنترل کند, مرورگر, یک فریم از پروتکل TCP/IP را به گذرگاه می فرستد, آدرس منبع فریم, آدرس PC's IP است, و آدرس مقصد, آدرس IP گذرگاه است, اطلاعات آدرس و دستکاری در آیتم های داده فریم ذخیره می شوند. زمانی که گذرگاه, فریم پروتکل TCP/IP را دریافت می کند, بسته ها را بر اساس این فرمت پروتکل باز می کند و داده های لایه برنامه را می گیرد. سپس, گذرگاه, این داده ها را مطابق با فرمت پروتکل پروفیباس بسته بندی می کند. حال آدرس منبع فریم پروتکل پروفیباس, آدرس پروفیباس گذرگاه است, آدرس مقصد, آدرس پروفیباس وسیله است. بنابراین داده هایی که توسط فرمت پروتکل پروفیباس بسته بندی می شوند, قابل انتقال به پروفیباس هستند. در مقابل, زمانی که پاسخ وسیله به درخواست گذرگاه صورت می گیرد, وسیله, داده ها را در فریم پروتکل پروفیباس به گذرگاه می فرستد, آدرس منبع فریم, آدرس پروفیباس وسیله است, آدرس مقصد, آدرس پروفیباس گذرگاه است, گذرگاه, بسته ها را مطابق با فرمت پروتکل پروفیباس باز می کند و سپس داده ها را مطابق با فرمت پروتکل TCP/IP بسته بندی می کند. آدرس منبع فریم بسته بندی شده, آدرس IP گذرگاه است, آدرس مقصد, آدرس PC's IP است. بنابراین, داده هایی که توسط فرمت پروتکل TCP/IP بسته بندی می شوند, قابل انتقال به اینترنت هستند. دیاگرام اصل تبدیل پروتکل در شکل 3 نشان داده شده است [3].



شکل 2. تبدیل آدرس



شکل 3. اصل تبدیل پروتکل پروفیباس و TCP/IP

B. تایید هویت و کنترل دسترسی اجباری

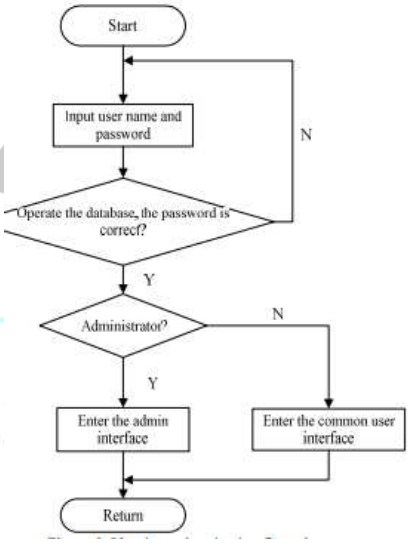
برای حصول اطمینان از شبکه پروفیباس, اولین چیز که باید در نظر گرفته شود, جلوگیری از دسترسی غیرقانونی است. تنها کاربران مجاز می توانند اجازه دسترسی به سیستم پروفیباس را داشته باشند. این مقاله, ایده کنترل دسترسی اجباری را اتخاذ می کند. اجازه قانونی کاربر برای دسترسی از راه دور توسط خودش تعیین نمی شود. سیستم کلی دارای یک مدیر ارشد است. مدیر ارشد, اجازه های قانونی را برای تمام منابع به طور یکنواخت تعیین می کند و یک برچسب را برای تمام کاربران و منابع اختصاص می دهد. برچسب ها شامل اجازه های قانونی مدیر و کاربر عادی می شوند. مدیر, مجاز به دیدن حالت وسیله و وسیله کنترل است, کاربر عادی تنها می تواند حالت وسیله را ببیند. در این مقال, فناوری پایگاه داده تعبیه شده و فناوری صفحه وب دینامیک- CGI برای تحقق تایید هویت و کنترل دسترسی استفاده می شوند.

اطلاعات داده ها, مهمترین اطلاعات در شبکه کنترل صنعتی است. و فناوری پایگاه داده به طور گسترده برای سازماندهی و ذخیره داده و همچنین بازیابی و پردازش داده ها با سرعت بالا استفاده می شود. نقش پایگاه داده در این طرح عمدتاً دو جنبه دارد. اولاً, برای مدیریت اطلاعات کاربر استفاده می شود. ثانیاً, برای حفظ تعداد زیادی از داده های به اشتراک گذاشته شده از وسایل استفاده می شود. به منظور اطمینان از عملکرد زمان واقعی, اطلاعات کنترل را می توان به طور مستقیم به وسایل صادر نمود و نه توسط پایگاه داده. با پیشرفت فناوری تعبیه شده, فناوری پایگاه داده تعبیه شده نیز, از مرحله پژوهش, پا به مرحله کاربرد وسیع از می گذارد. SQLite, یک پایگاه داده تعبیه شده سبک است, منابع کمی را اشغال می کند و از سیستم عامل لینوکس و زبان برنامه نویسی C پشتیبانی می کند. در عین حال, دارای سرعت پردازش بالاست. SQLite در این طرح برای خلق یک پایگاه داده اجازه قانونی, استفاده می شود, این پایگاه داده, شامل نام کاربرد, رمز عبور متناظر و اجازه قانونی کاربر می شود. در حالیکه واسطه ورود طراحی شده, اجازه قانونی کاربر را نمایش نمی دهد, تنها حوزه ورودی نام و رمز عبور کاربر را نشان می دهد. این امر, محرمانگی اطلاعات را تضمین می کند و از حمله کاربران غیرقانونی به سیستم جلوگیری می کند. مثلاً, زمانی که کاربران غیرقانونی از این مورد آگاه می شوند که این سیستم دارای اجازه مدیر از طریق صفحه ورودی است, آنها ممکن است حمله ای را برای ورود به سیستم انجام دهند. زمانی که آنها به طور موفقیت آمیز وارد می شوند و به طور غیرقانونی با تجهیزات کار می کنند, عملیات نرمال تجهیزات مغشوش خواهد شد و حتی سبب یک آسیب مرگبار به تجهیزات می شود. پایگاه داده خلق شده اجازه قانونی در شکل 4 نشان داده شده است.

```
sqlite> .mode column
sqlite> .header on
sqlite> select *from tb1;
username    password    authority
----------  ----------  ----------
chaidan     3141846     guanliyuan
liming      2354321     putongyong
wanglong    1234567     putongyong
sqlite>
```

شکل 4. پایگاه داده اجازه قانونی

واسطه گذرگاه مشترک (CGI) یک واسطه استاندارد برای تعامل برنامه گسترش خارجی با سرور وب است, زمانی که سرور وب مشخص می کند که درخواست فرستاده شده توسط مرورگر متقاضی, یک برنامه CGI است و نه یک صفحه HTML ساده نرمال, سرور وب, برنامه CGI را فعال خواهد ساخت. [4] در فرآیند نظارت بر تجهیزات صنعتی, برنامه نرم افزار CGI متناظر برای خواندن اطلاعات کاربر که توسط کاربر در بروشور وارد شده است استفاده می شود. در همین زمان, برنامه CGI, پایگاه داده اجازه قانونی را به راه می اندازد و سطح اجازه و دسترسی کاربر را تعیین می کند. اگر کاربر مجاز نشود, گذرگاه, دسترسی کاربر به سیستم را ممنوع می کند. در حالیکه اگر کاربر مشروع باشد, برنامه CGI, تعیین می کند که آیا کاربر مدیر است یا کاربر عادی, و سپس مطابق با اجازه کاربر, به واسطه کاربر متناظر باز می گردد. شکل 5, فلوچارت تایید هویت را نشان می دهد.



شکل 5. فلوچارت تایید هویت

C. امنیت انتقال داده ها

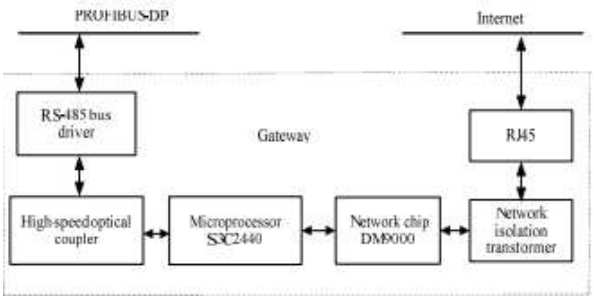
اطلاعات کاربر و اطلاعات تجهیزات, به صورت متن در شبکه منتقل می شوند, اگر هیچ عملیات پردازش مخفی کاری داده ها اتخاذ نشده باشد, کاربران غیرقانونی می توانند اطلاعات کاربر و اطلاعات تجهیزات را بگیرند و این کار را با استفاده از نرم افزار ضبط شبکه انجام می دهند و حتی در داده های تجهیزات فضولی نمایند که این یک مسئله امنیتی وحشتناک است, بنابراین این اطلاعات باید قبل از انتقال رمزگذاری شوند.

پروتکل SSL (لایه سوکت امن), نوعی از پروتکل ایمنی است که خدمات محرمانه را بر اساس اینترنت فراهم می کند و بین لایه انتقال و لایه نرم افزار کار می کند. و سه مشخصه را برای کانال امن فراهم می کند: محرمانگی, قطعیت, قابلیت اطمینان [5]. در این مقاله, فناوری وب تعبیه شده برای تحقق تعامل بین متقاضی و وسایل استفاده می شود و پروتکل لایه نرم افزار, پروتکل HTTP است. مرورگرهای جریان اصلی جاری مانند اینترنت اکسپلورر و SSL Firefox Support هستند. سرور appweb انتخاب شده در این مقاله, از SSL حمایت می کند. بنابراین ما باید پروتکل SSL تعبیه شده را در گذرگاه تعبیه شده قرار دهیم و SSL را در فایل پیکربندی سرور Appweb فعال سازیم. زمانی که HTTP برای برقراری ارتباط بر اساس پروتکل SSL, نام کاربرد, رمز عبور استفاده می شود و داده های کنترل به بخشی از جریان رمزگذاری شده داده های SSL تبدیل شده اند, بسته های فرستاده شده روی اینترنت, نشست نمی کنند, استراق نمی شوند, تداخل ندارند و پنهان نمی شوند. به طور مشخص, این روش عمدتاً موجب ساده شدن فرایند توسعه می شود, چرخه توسعه را کاهش می دهد و در عین حال, ایمنی انتقال داده ها را تضمین می کند.

IV. تحقق گذرگاه وب امن تعبیه شده

A. طراحی سخت افزاری

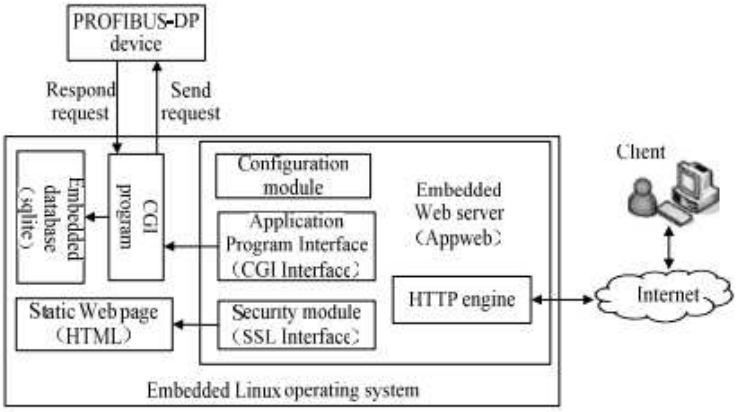
ساختار ساخت افزاری گذرگاه وب تعبیه شده در شکل 6 نشان داده شده است [3]. بسته ها از اینترنت به پردازشگر ARM S3C2440 توسط Rj45, ترانسفورمر ایزولاسیون شبکه و تراشه شبکه DM9000 منتقل می شوند. بسته ها از PROFIBUS-DP به پردازشگر ARM S3C2440 از طریق درایور باس RS-485 منتقل می شوند. پردازشگر S3C2440 مسئول پردازش داده های منتقل شده بین اینترنت و PROFIBUS-DP است.



شکل 6. ساختار گذرگاه وب تعبیه شده

B. پیاده سازی نرم افزار

سیستم عامل تعبیه شده لینوکس, روی سیستم عامل تعبیه شده گذرگاه گذاشته می شود. برای ارائه حفاظت امنیتی, سرور Appweb تعبیه شده, SLite پایگاه داده تعبیه شده و پروتکل SSL تعبیه شده Matrixssl روی آن قرار داده می شوند. معماری نرم افزاری گذرگاه وب تعبیه شده به صورت شکل 7 می باشد.



شکل 7. معماری نرم افزاری گذرگاه وب تعبیه شده

1) پیاده سازی تایید هویت و کنترل دسترسی

صفحه ورود در زبان HTML نوشته می شود و در دایرکتوری www/ از سیستم فایل ذخیره می شود. مسیر دسترسی پیش فرض www/ را در فایل پیکربندی سرور تنظیم نمایید. زمانی که کاربران وارد آدرس IP از گذرگاه در مرورگر می شود, واسطه ورود نمایش داده خواهد شد. کاربران, نام و رمز عبور کاربری را در صفحه ورودی وارد می کنند, واسطه CGI از سرور, برنامه CGI را برای تایید هویت کاربر فراخوانی می کند. آدرس IP گذرگاه 192.168.1.230 را در مرورگر وارد کنید, صفحه ورودی پدیدار می شود, که در شکل 8 نشان داده شده است.

شکل 8. تحقق امنیت انتقال داده ها

شکل 9. بسته ضبط شده با استفاده از پروتکل SSL

به منظور آزمایش اعتبار پروتکل SSL طراحی شده در ماژول امنیتی, نرم افزار ضبط شبکه Iris, برای ترکیب بسته ها استفاده می شود.

جملاتی را برای فعال نمودن ماژول SSL در فایل پیکربندی سرور Appweb بیافزایید و به پورت سرور وب 443 به روشی ایمن دست یابید, "https://192.168.1.230" را در مرورگر وارد کنید. همانطور که در شکل 9 نشان داده شده است, می توانیم ببینیم که داده ها رمزگذاری شده اند, و نمی توان به هیچ گونه اطلاعات مفیدی دست یافت.

V. نتیجه گیری

برای تحقق نظارت از راه دور, یک روش ارتباط بین اینترنت و شبکه PROFIBUS-DP بر اساس گذرگاه وب تعبیه شده, در این مقاله بیان شده است. برای الزام امنیتی شبکه صنعتی بر اساس PROFIBUS, چندین معیار امنیتی در زمان دسترسی شبکه PROFIBUS به اینترنت در این تحقیق پیشنهاد شده اند. تحلیل مکانیزم امنیتی و روش پیاده سازی روش تبدیل پروتکل بین PROFIBUS و TCP/IP طراحی می شود, و این مبنای عملیات امن وسیله PROFIBUS-DP توسط اینترنت است. مکانیزم کنترل دسترسی اجباری امن تایید هویت کاربر طراحی و پیاده سازی شده است. می توان تضمین نمود که تنها کاربران مجاز می توانند به منابع سیستم مجاز دسترسی داشته باشند. فناوری امنیتی SSL تعبیه شده نیز به طور خاص برای الزام امنیتی اتخاذ شده است و به گذرگاه وب تعبیه شده قرار داده شده است. با استفاده از این روش, پنهانی بودن و ایمنی بودن داده های اطلاعات کاربر و داده های تجهیزات را می توان به طور موثر در زمان دسترسی PROFIBUS-DP توسط اینترنت محافظت نمود. با دروازه وب امن تعبیه شده, مدیران و مهندسان می توانند تجهیزات و فرآیند تولید را در طول زمان, از راه دور, به طور ایمن و به طور موثر توسط اینترنت کنترل نمود. این موفقیت, اهمیت زیادی برای شرکت در کاهش هزینه تولید و تسریع توسعه شبکه و اطلاعاتی شدن صنعتی دارد و شبکه در پیکربندی شبکه شرکتی صنعتی امن و منسجم مفید است.

REFERENCES

[1] GUO Meng,, QIAN Jiang, "A Design of Security Model for Control Network of Industrial Ethernet", Microcomputer Information, 2008(11-3),pp.53-55.

[2] ZHAO Yuehua, DU Yunhai, BAO Mingguo, "Implementation of Security in Embedded Web Gate Based on Authentication", Computer Engineering,2004(23),pp.111-113.

[3] LiTing, "Research and Implementation of Remote Monitoring Methods Based on IPv6 and PROFIBUS",[D], Jilin University, 2013.

[4] CHEN Tian-huang, HUANG Jia-xi, " Design and Realization of CGI in Embedded Dynamic Web Technology", 2007 IFIP International Conference on Network and Parallel Computing – Workshops,2007,pp. 774-777.

[5] SHEN Yong, ZHU Chao, "Design and Implementation of Embedded Web Server Security Based on SSL", Computing Technology and Automation, 2012(7),pp. 160-162.