مراحل برقراری امنیت برای کل سامانه‌های موجود در طرح فهام

۱- تمهیدات امنیت پیش‌بینی شده برای سیستم‌های AMI:

همانگونه که مستحضر هستید امنیت یک موضوع اساسی در مخابرات و فناوری اطلاعات می‌باشد به طوریکه در چند سال اخیر توجه زیادی به امنیت سیستم‌های صنعتی که همزمان دارای پیچیدگی زیادی هستند، شده است.

در سال‌های اخیر تاکید زیادی بر حفاظت ساختارهای حیاتی سیستم‌های حسگر بی‌سیم و شبکه‌های اندازه‌گیری به خصوص ساختارهای مرتبط با انرژی، حمل و نقل و مخابراتی وجود دارد. مسائل امنیتی پیرامون سیستمهای اندازه‌گیری هوشمند نیز در این زمینه بسیار مورد توجه می‌باشند.

امنیت در سراسر فرآیند اندازه‌گیری از کنتور و DC گرفته تا CAS که شامل سیستم‌های سخت‌افزاری و نرم‌افزاری فراوانی می‌باشد باید مورد توجه قرار گیرد. همچنین به دلیل وجود ارتباطات گسترده بین مولفه‌های سیستم، نیازمند امنیت سراسری می‌باشیم. از اینرو، کلیه عوامل از جمله سازندگان، تامین‌کنندگان و قانون‌گذاران جهت افزایش سطح آگاهی و تضمین امنیت سیستم‌های اندازه‌گیری در آینده باید با یکدیگر مشارکت نمایند. در ادامه بصورت اجمالی به مشخصات امنیتی ویژه کنتورهای هوشمند پرداخته می‌شود همچنین بصورت فهرست‌وار اساس طراحی امنیت و مهمترین موارد جهت تامین محرمانه بودن اطلاعات در سیستمهای اندازه‌گیری هوشمند ارایه می‌شود.

۱-۱ مشخصات امنیتی در کنتورهای هوشمند

- استفاده از واسط‌های ارتباطی استاندارد برای ارتباط کنتور و ماژول مخابراتی (که در سند الزامات عمومی، اقتصادی، عملکردی، فنی و مخابراتی فراسامانهٔ هوشمند اندازه‌گیری و مدیریت انرژی (فهام) لحاظ شده است.)
- استفاده از پروتکل استاندارد یکسان برای جابجایی داده (بحث interoperability که در مرحله اول طرح فهام نهایی خواهد شد.)
- امنیت تبادل اطلاعات بصورت ارتباطات دوطرفه (Two way communications) (که کمیته امنیت طرح فهام متولی برقراری امنیت در تمام قسمتهای سیستم است)

۱-۲ اساس طراحی امنیت

- محرمانه بودن : اطمینان از اینکه اطلاعات فقط توسط افراد مجاز، مورد استفاده قرار می‌گیرد.
- یکپارچگی : حراست از دقیق و کامل بودن اطلاعات و روش های پردازشی.
- در دسترس بودن : اطمینان از اینکه کاربران مجاز به اطلاعات دسترسی دارند.
- احراز اصالت: اطمینان از اینکه فقط کاربران مجاز به اطلاعات دسترسی دارند.

۱-۳ موارد مهم جهت تامین محرمانه بودن اطلاعات

- حفاظت منابع با ارزش به وسیله محدود کردن دسترسی
- شناخت نفوذ
- مکانیسم جلوگیری از نفوذ
- قابل به روز کردن تنظیمات اندازه‌گیری و پیکربندی و تعریف سطوح امنیتی تجهیزات AMI به صورت از راه دور.
- رمزنگاری

۱-۴ شیوه‌های مختلف و متداول رمزنگاری اطلاعات

گسترش و رشد بی‌سابقه ارتباطات باعث ایجاد تغییرات گسترده در نحوه زندگی و فعالیت شغلی افراد، سازمانها و موسسات شده است . امنیت اطلاعات یکی از مسائل مشترک شخصیت های حقوقی و حقیقی است. کاربران شبکه‌های ارتباطی در زمان استفاده از شبکه، اطلاعات حساس و مهمی را بدفعات ارسال و یا دریافت می‌دارند. اطمینان از عدم دستیابی افراد غیر مجاز به اطلاعات حساس از مهمترین چالش های امنیتی در رابطه با توزیع اطلاعات از طریق شبکه‌های بی‌سیم است. در این قسمت به معرفی انواع روشها و الگوریتمهای مختلف رمزنگاری اطلاعات می‌پردازیم برای این کار نیاز است تا اطلاعات حساس سیستم‌های اندازه‌گیری هوشمند که تمایلی به مشاهده آنان توسط دیگران نیست، را طبقه‌بندی کنیم. برخی از اطلاعات بشرح زیر است:

- اطلاعات مصرف مشترکین
- سریال مربوط به کنتورهای آب، برق و گاز
- اطلاعات خصوصی مشترکین که حاوی میزان مصرف انرژی است
- جزئیات اطلاعات شخصی (حضور یا عدم حضور در منزل، نوع وسایل مصرفی، هزینه‌های مصرفی و ...)
- اطلاعات حساس مصرف انرژی در یک سازمان خاص
- اطلاعات مربوط به قبض‌های انرژی

تاکنون برای امنیت اطلاعات بر روی شبکه‌های کامپیوتری و یا اینترنت از روش‌های متعددی استفاده شده است. ساده‌ترین روش حفاظت از اطلاعات نگهداری اطلاعات حساس بر روی محیط‌های ذخیره‌سازی قابل انتقال نظیر فلاپی دیسک‌ها و فلش‌ها است. متداولترین روش حفاظت اطلاعات، رمز نمودن آنها است. این عمل بدین منظور انجام می‌شود تا دستیابی به اطلاعات رمز شده برای افراد غیرمجاز امکان‌پذیر نبوده و صرفاً افرادیکه دارای کلید رمز هستند، قادر به باز نمودن رمز و استفاده از اطلاعات آن هستند.

رمز نمودن اطلاعات شبکه مبتنی بر علوم رمزنگاری است. استفاده از علم رمزنگاری دارای یک سابقه طولانی و تاریخی است. قبل از عصر اطلاعات، بیشترین کاربران رمزنگاری اطلاعات توسط دولت‌ها و در موارد نظامی بوده است. سابقه رمز نمودن اطلاعات به دوران امپراطوری روم باز می‌گردد. امروزه اغلب روش‌ها و

مدل‌های رمزنگاری اطلاعات در رابطه با کامپیوتر بخدمت گرفته می‌شود. کشف و تشخیص اطلاعاتی که بصورت معمولی در حافظه کامپیوترها ذخیره و فاقد هر گونه روش علمی رمزنگاری قوی باشند، براحتی و بدون نیاز به تخصصی خاص انجام خواهد شد.

اکثر سیستم‌های رمزنگاری اطلاعات در شبکه‌های داده به دو گروه عمده زیر تقسیم می‌گردند:

- رمزنگاری کلید- متقارن
- رمزنگاری کلید– عمومی (نا متقارن)

۱-۴-۱ رمزنگاری کلید - متقارن

در روش فوق، هر کامپیوتر دارای یک کلید رمز (کد) بوده که از آن برای رمزنگاری یک بسته اطلاعاتی قبل از ارسال اطلاعات بر روی شبکه و یا کامپیوتر دیگر، استفاده می‌نماید. در این روش لازم است در ابتدا مشخص گردد که کدام یک از نودهای شبکه قصد تبادل اطلاعات با یکدیگر را دارند، پس از مشخص شدن هر یک از آنها، در ادامه کلید رمز بر روی هر یک از سیستمها باید نصب گردد. اطلاعات ارسالی توسط کامپیوترهای فرستنده با استفاده از کلید رمز، رمزنگاری شده و سپس اطلاعات رمز شده ارسال خواهند شد. پس از دریافت اطلاعات رمز شده توسط کامپیوترهای قسمت گیرنده، با استفاده از کلید رمز اقدام به بازگشائی رمز و برگرداندن اطلاعات بصورت اولیه و قابل استفاده خواهد نمود. در صورتیکه گیرنده پیام دارای کلید رمز مناسب نباشد، قادر به رمزگشائی و استفاده از اطلاعات نخواهد بود. گیرنده پیام با انجام عملیات معکوس قادر به شکستن رمز و استفاده از اطلاعات خواهد بود.

از جمله به روزترین و معتبرتین الگوریتم‌های رمزنگاری متقارن، الگوریتم AES با طول کلید ۱۲۸ بیت می‌باشد که تا این لحظه کسی قادر به شکستن قفل این رمزگذاری نشده است.

۱-۴-۲ رمزنگاری کلید - عمومی

در روش فوق از ترکیب یک کلید خصوصی و یک کلید عمومی استفاده می‌شود. کلید خصوصی صرفاً متعلق به سیستم فرستنده بوده و کلید عمومی توسط کامپیوتر فرستنده در اختیار هر یک از کامپیوترهائی که قصد برقراری ارتباط با یکدیگر را دارند، به اشتراک گذاشته می‌شود. برای رمزگشائی یک پیام رمز شده، کامپیوتر مقصد باید از کلید عمومی که توسط فرستنده ارسال شده، به همراه کلید خصوصی خود استفاده نماید. یکی از متداولترین برنامه‌های رمزنگاری در این رابطه **رمزنگاری** Elliptic Curve Cryptography (ECC) است. با استفاده از ECC می توان هر متن دلخواهی را با سرعت قابل قبولی رمز نمود.

به منظور پیاده‌سازی رمزنگاری مبتنی بر کلید- عمومی در مقیاس بالا نظیر یک سرویس دهنده بزرگ شبکه هوشمند برق، لازم است از رویکردهای دیگری در این خصوص استفاده گردد. «امضای دیجیتال» یکی از رویکردهای موجود در این زمینه است. یک امضای دیجیتالی صرفاً شامل اطلاعات محدودی بوده که اعلام می‌نماید، سرویس دهنده شبکه با استفاده و بکارگیری یک سرویس مستقل با نام «امضای مجاز»، حق دسترسی

به اطلاعات مشخصی را دارد. «امضای مجاز» بعنوان یک میانجی بین دو سیستم فرستنده و گیرنده ایفای نقش می‌نماید. هویت و مجاز بودن هر یک از سیستم‌ها برای برقراری ارتباط توسط سرویس‌دهنده انجام و برای هر یک کلید عمومی مربوطه را فراهم خواهد کرد.

به عنوان مثال یکی از متداولترین نمونه‌های پیاده‌سازی شده در شبکه اینترنت مبتنی بر رمزنگاری کلید-عمومی، روش Secure Sockets Layer (SSL) است. SSL یک پروتکل امنیتی اینترنت بوده که توسط مرورگرها و سرویس دهندگان وب‌های مختلف بمنظور ارسال اطلاعات حساس، استفاده می گردد. استفاده از پروتکل "https" در عوض پروتکل "http" یکی از روش های موجود است.

مشکل عمده رمزنگاری‌های مبتنی بر کلید- عمومی، مدت زمان زیادی است که سیستم صرف انجام محاسبات می‌نماید. بنابراین در اکثر سیستم‌ها از ترکیب کلید عمومی(نامتقارن) و متقارن استفاده می‌گردد. زمانیکه دو نود مختلف یک ارتباط امن را با یکدیگر برقرار می‌نمایند، یکی از سیستم‌ها یک کلید متقارن را ایجاد و آن را برای کامپیوتر دیگر با استفاده از رمزنگاری کلید- عمومی(نامتقارن)، ارسال خواهد کرد. در ادامه دو سیستم گیرنده و فرستنده قادر به برقراری ارتباط به کمک رمزنگاری کلید متقارن می‌شوند. پس از اتمام ارتباط، هر یک از سیستم‌ها کلید متقارن استفاده شده را دور انداخته و در صورت نیاز به برقراری یک ارتباط مجدد، باید مجدداً فرآیند فوق تکرار گردد (ایجاد یک کلید متقارن، ....)

۱-۵ احراز اصالت:

همانگونه که در ابتدای بخش قبلی اشاره شد، رمزنگاری فرآیندی است که براساس آن اطلاعات ارسالی از یک نود(گره) برای نود دیگر، در ابتدا رمز و سپس ارسال خواهند شد. گره دوم یا همان گیرنده، پس از دریافت اطلاعات باید، اقدام به رمزگشائی آنان نماید. یکی دیگر از فرآیندهای موجود بمنظور تشخیص ارسال اطلاعات توسط یک منبع امن و مطمئن، استفاده از روش معروف «احراز اصالت» است. در صورتیکه اطلاعات «معتبر» باشند، شبکه نسبت به هویت ایجاد کننده اطلاعات آگاهی داشته و این اطمینان را بدست خواهد آورد که اطلاعات از زمان ایجاد تا زمان دریافت توسط شما تغییری پیدا نکرده است. با ترکیب فرآیندهای رمزنگاری و احراز اصالت می‌توان یک محیط امن را ایجاد کرد.

مجموعه تدابیر امنیتی فوق در پروتکل DLMS/COSEM پیش‌بینی شده است.

۲- اقدامات امنیتی در زمان اجرا

با استفاده از گواهینامه‌ها، امکانات ایجاد خدمات امنیتی از قبیل احراز اصالت، یکپارچگی، قابلیت اعتماد، ایجاد برچسب زمانی یا انکار ناپذیری[1] امکانپذیر می‌گردد. تمام طول کلید باید در طول عمر یک سیستم استفاده شود. استفاده از RSA-2048 برای سیستم‌هایی اندازه‌گیری هوشمند که ما بین سالهای ۲۰۱۱ تا

[1] Non-repudiation

۲۰۲۰ پیاده‌سازی خواهند شد، توصیه می‌گردد. طول کلید باید بر مبنای آخرین استانداردهای بین‌المللی انتخاب شود.

ایجاد و پیاده‌سازی یک معماری با استفاده از کلیدهای خصوصی و عمومی بسیار مهم است و استفاده از RSA[۲]، AES[۳] و الگوریتم‌های متقارن و نامتقارن با بهترین و امن‌ترین طول کلید باید برای شبکه LAN عملی گردد. بعلاوه، استفاده از الگوریتم رمزنگاری ECC[۴] با طول کلید ۱۹۲ بیت نیز می‌تواند امنیت قابل قبولی در سطح شبکه WAN برقرار سازد. همچنین در ارتباط با بستر مخابراتی مناسب امر شبکه هوشمند اندازه‌گیری برق، پیروی بررسی‌ها و تحقیقاتی که مشاور فنی طرح فهام به عمل آورده است، بستر مخابراتی PLC و RF را برای شبکه LAN و بستر مخابراتی GPRS و WiMAX را برای شبکه WAN به عنوان بهترین گزینه موجود معرفی نمودند. با توجه به اینکه کار بصورت کلید تحویل شامل طراحی، تامین، نصب و بهره‌برداری محدود به پیمانکار EPC واجد شرایط واگذار خواهد شد، این پیمانکار باید شرکت ارائه‌دهنده سرویس عمومی شبکه WAN که دارای مجوز فعالیت از وزارت ارتباطات و فناوری اطلاعات است را به عنوان همکار به خدمت بگیرد و بستر مخابراتی LAN توسط تامین کننده کنتور و سیستم هوشمند فراهم خواهد شد. در مدت زمان اجرای پروژه نیز مشاور فنی طرح فهام نظارت دقیقی بر کلیه ساختار و جزئیات پیاده‌سازی این سیستم خواهد داشت.

در همین راستا جهت بذل توجه حداکثری به مقوله امنیت، کمیته‌ای با نام کمیته امنیت طرح فهام در سازمان بهره‌وری انرژی ایران تشکیل شده است. این کمیته برآیندی از نخبگان بومی بحث‌های مخابراتی و IT است که از سازمان‌های دولتی زیر دستچین شده‌اند:

۱- سازمان پدافند غیرعامل
۲- انجمن رمز ایران
۳- پژوهشگاه الکترونیک دانشگاه صنعتی شریف
۴- کمیته IT شرکت توانیر
۵- دفتر حراست و امور محرمانه شرکت توانیر
۶- کنسرسیوم تولیدکنندگان کنتور برق ایران
۷- معاونت سیستم‌های اندازه‌گیری و شبکه هوشمند سابا

از طریق این کمیته براساس دو سند بالادستی موجود افتا و سماد، ساز و کار لازم برای تهیه و تدوین سند الزامات امنیتی طرح فهام پیاده شده و ضمن برگزاری جلسات دوره‌ای منظم تهدیدات و مخاطرات امنیتی احتمالی را که در آینده سیستم AMI با آنها مواجه خواهد شد را شناسایی کرده و با ارایه راهکاری بومی و عملیاتی سعی در رفع موارد مذکور می‌نماید.

[2] -Rivets, Shamir& Adleman
[3] -Advanced Encryption Standard
[4] -Elliptic Curve Cryptography

۳- آزمایشات پیشنهادی راستی‌آزمایی برای تشخیص میزان امنیت

از آنجا که برقراری امنیت مقوله‌ای پویا و بلاتوقف است، پس از بررسی‌های فراوان در این خصوص یکی از بهترین راهکارها جهت شناخت میزان امنیت سیستم AMI و افزایش مداوم آن به تمام شرکت‌های خدمات‌رسان انرژی و فروشنده‌ها این است که آزمایش‌های امنیتی زیر را به‌طور منظم انجام و نقاط قوت و ضعف سیستم را تشخیص دهند همچنین تدوین این آزمایشات و نحوه اندازه‌گیری و اعمال آنها نیز از دیگر وظایف کمیته امنیت طرح فهام است که با توجه به تفاهم‌نامه مشترکی که بین سابا و پژوهشگاه نیرو وجود دارد، آن نهاد وظیفه انجام آزمایشات و دادن گواهینامه‌های مربوطه را برعهده دارد. هرگاه آزمایش امنیتی خاصی مورد نیاز بود که پژوهشگاه از امکانات و دانش فنی لازم آن برخوردار نبود موظف است آزمایشگاه معتبر داخلی یا خارجی را برحسب مورد معرفی و تجهیزات را جهت تست به آن مرکز ارسال نماید. لیست برخی از مهمترین آزمایشات امنیتی در زیر آمده است:

۱) تست‌های نفوذ در لایه‌های امنیت فیزیکی
۲) تست‌های نفوذپذیری سیستم حفظ تمامیت اطلاعات
۳) تست‌های سیستم‌های متراکم محاسبات داده‌های رسیده از DC
۴) تست‌های سیستم‌های جمع‌کننده داده‌ها DC

۴- نتیجه‌گیری

با توجه به جمیع تمهیدات امنیتی پیش‌بینی شده برای نصب و راه‌اندازی سیستمهای اندازه‌گیری هوشمند و همچنین نظارت دائمی و منظم کمیته امنیت طرح فهام به همراه اعضای محترم سازمان پدافند غیرعامل و حراست توانیر و سایر اعضای آن قطعاً کنتورهای هوشمندی که پس از انجام آزمونهای امنیتی مجوزهای لازم رای برای نصب در محل مشترکین کسب نموده‌اند بدون مشکل امنیتی کار کنند و امنیت سیستم اندازه‌گیری هوشمند انرژی در سطح قابل قبولی برقرار شود. لازم به ذکر است این طرح جزو معدود طرحهای ICT صنعت برق می‌باشد که از ابتدای مرحله مطالعات و طراحی به مقوله امنیت و پدافند غیرعامل بصورت جدی و سازماندهی شده پرداخته است که البته توجهات و تذکرات بموقع حراست شرکت توانیر، سازمان پدافند غیرعامل و کمیته پدافند غیرعامل شرکت توانیر در این زمینه نقش بسزایی داشته است.