امنیت اطلاعات در سیستم‌های اندازه‌گیری هوشمند و طرح فهام

میثم رضاییان[۱]، هادی مدقق[۲]، نادر سالک گیلانی[۳]
معاونت سیستم‌های اندازه‌گیری و شبکه هوشمند
سازمان بهره‌وری انرژی ایران(سابا)
تهران، ایران
rezaeian@saba.org.ir [1], modaghegh@saba.org.ir[2], salek@saba.org.ir [3]

چکیده – در سال‌های اخیر با توسعه سامانه‌های اطلاعاتی و رایانه‌ای، مسئله امنیت اطلاعات بطور ویژه‌ای مورد توجه قرار گرفته است. با توجه به پیاده‌سازی سیستم اندازه‌گیری هوشمند(AMI) در آینده‌ای نزدیک شرکت‌های توزیع نیروی برق قادر خواهند بود مدیریت و نظارت بر مشترکین خود را از راه دور بواسطه این سیستم انجام دهند و از سوی دیگر امکان تعامل کلیه مشترکین با این شرکت‌ها فراهم خواهد گردید. مسئله اساسی، بحث امنیت سیستم اندازه‌گیری هوشمند و چگونگی مدیریت و تبادل داده آن خواهد بود که به طور مستقیم فعالیت‌های حیاتی این سیستم را تحت شعاع خود قرار می‌دهد. بنابراین می‌توان با سرمایه‌گذاری منطقی در امنیت اطلاعات و پیاده‌سازی یک سیستم مدیریت امنیت اطلاعات منسجم و در نظر گرفتن مکانیزم‌های امنیتی مناسب از مزایای افزایش قابلیت اطمینان سیستم، تداوم فعالیت شبکه، کاهش تهدیدات امنیتی و اثرات آنها و افزایش رضایت‌مندی مشترکین در کنار مزایای دیگر سیستم اندازه‌گیری هوشمند بهره برد. در این مقاله به مباحث پیرامون امنیت اطلاعات در سیستم‌های اندازه‌گیری هوشمند شامل تهدیدات، سرویس‌ها و مکانیزم‌های امنیتی برای مقابله با مخاطرات سیستم پرداخته و به طور خاص راهکارها و کنترل‌های پیشنهاد شده در طرح فراسامانه هوشمند اندازه‌گیری و مدیریت انرژی(فهام) ایران بیان شده است.

واژه‌های کلیدی – امنیت اطلاعات، سیستم‌های اندازه‌گیری هوشمند، سیستم مدیریت امنیت اطلاعات، مدیریت مخاطرات، گوهر، مرکز امنیت اطلاعات، سیستم مدیریت کلید، رمزنگاری، الگوریتم کلید عمومی، فراسامانه هوشمند اندازه‌گیری و مدیریت انرژی(فهام).

۱. امنیت اطلاعات

امنیت اطلاعات[۱] (InfoSec) به حفاظت از اطلاعات بدون در نظر گرفتن فرم اطلاعات (اعم از الکترونیکی، فیزیکی و...) در مقابل دسترسی‌های غیرمجاز، سوءاستفاده، افشا، اختلال، تغییر، خواندن، ضبط و تخریب گفته می‌شود. امنیت اطلاعات با هدف تضمین استمرار فعالیت‌های جاری، به حداقل رساندن مخاطره‌های آن و افزایش میزان بازده سرمایه‌گذاری‌ها و فرصت‌ها صورت می‌پذیرد.

تاریخچه امنیت اطلاعات با تاریخچه امنیت رایانه آغاز می‌شود. با شروع جنگ جهانی دوم، اولین رایانه‌های بزرگ برای شکستن کدهای امنیتی توسعه یافتند. در آن زمان نیاز امنیتی در حفاظت از اماکن، تجهیزات و نرم‌افزارها از تهدیدات خارجی خلاصه می‌شد و این دیدگاه فنی از امنیت تا اوایل دهه ۱۹۸۰ میلادی مطرح بود[۱]، اما با گذشت زمان مشخص گردید که بیشتر تجاوزات امنیتی از طریق مسائلی همچون ضعف‌های مدیریتی از لحاظ امنیتی و عوامل انسانی بدلیل عدم آموزش‌های امنیتی پرسنل سازمان مربوطه می‌باشد، لذا از اواسط دهه ۸۰ تا اواسط دهه ۹۰ میلادی، بحث مدیریت امنیت اطلاعات مطرح شد که در آن امنیت اطلاعات را منوط به خطی مشی امنیت اطلاعات و ساختارهای سازمانی می‌دانستند. در اواسط دهه ۹۰ میلادی این مباحث کامل‌تر گردید که آمیزه‌ای از دو مرحله قبلی و پارامترهای دیگری همچون تعریف سیاست‌ها و مکانیزم‌های امنیتی بر اساس نیازهای اصلی سازمان و مدیریت آن بود. این مرحله شامل مولفه‌هائی نظیر استانداردسازی امنیت اطلاعات، گواهینامه‌های بین‌المللی، فرهنگ‌سازی امنیت اطلاعات در سازمان و پیاده‌سازی معیارهای ارزیابی دائمی و پویای

[1] Information Security

امنیت اطلاعات است که این روند همچنان ادامه داشته و در حال تکمیل‌شدن می‌باشد[۲]. امروزه نیز اینترنت، ارتباط مستمر میلیون‌ها شبکه‌های رایانه‌ای ناامن را به یکدیگر برقرار می‌نماید. افزایش حملات سایبری، شرکت‌ها و دولتمران را ملزم به حفاظت از سیستم‌های کنترل‌شده با رایانه در صنایع عمومی و دیگر زیرساخت‌ها حیاتی نموده است که نشان‌دهنده اهمیت امنیت اطلاعات در سطح امنیت ملی می‌باشد.

یک شبکه توزیع هوشمند، دارای یک سیستم اطلاعاتی و نظارتی یکپارچه است که می‌تواند هر یک از تجهیزات متصل به شبکه را نظارت و مدیریت نماید. اطلاعات دریافتی و فرمان‌های ارسالی به کنتورها و منابع تولید پراکنده و دیگر تجهیزات در سطح مصرف کننده در شبکه توزیع هوشمند با استفاده از سیستم اندازه‌گیری هوشمند(AMI) فراهم می‌گردد. در سیستم اندازه‌گیری هوشمند همانند دیگر سیستم‌های اطلاعاتی، نگرانی‌هایی در مورد مسائل امنیتی وجود دارد. برای مثال ممکن است در صورت عدم رعایت اصول امنیتی، داده‌های قرائت شده کنتور دستکاری گردد یا با شنود اطلاعات اندازه‌گیری و تشخیص زمان‌های مصرف پیک توسط هکرها، زمان حضور مشترکین در منازل فاش گردد و یا به جهت اینکه کنتورها به شبکه هوشمند متصل می‌باشند در صورت حمله به سیستم و قطع به یکباره تعداد زیادی از مشترکین، تامین انرژی و تعادل بار در کل شبکه تحت تاثیر قرار گیرد. بنابراین باید با ملاحظات امنیتی مناسب، در جهت کنترل و مقابله با تهدیدات امنیتی بالقوه بکارگیری کنتورهای هوشمند اقدام نمود.

در این مقاله، در ابتدا به معرفی سیستم مدیریت امنیت اطلاعات و یکی از استانداردهای شاخص موجود و مراحل ایجاد این سیستم می‌پردازیم. سپس به سرویس‌ها، تهدیدات و مکانیزم‌های امنیتی پرداخته و به طور خاص نیز راهکارها و مکانیزم‌های امنیتی در طرح فهام پرداخته می‌شود.

۲.سیستم مدیریت امنیت اطلاعات(ISMS)

اطلاعات همانند سایر دارائی‌ها به عنوان یک دارائی مهم و با ارزش برای هر سازمان به حساب می‌آید و در نتیجه نیازمند ارائه راهکارهای حفاظتی لازم برای نگهداری از آنها می‌باشند. برای برقراری امنیت اطلاعات و مدیریت اطلاعات حساس یک سازمان از مجموعه‌ای از سیاست‌ها و طرح‌ریزی فعالیت‌ها، مسئولیت‌ها، فرآیندها و مکانیزم‌های امنیتی استفاده می‌گردد که به آن سیستم مدیریت امنیت اطلاعات[۲](ISMS) گفته می‌شود. سیستم مدیریت امنیت اطلاعات استانداردهایی را برای ایمن‌سازی فضای تبادل اطلاعات در سازمان‌ها ارائه می‌دهد و هدف آن ایجاد، پیاده‌سازی، اجرا، پایش، بازبینی، نگهداری و بهبود امنیت اطلاعات با طرح مخصوص به آن سازمان است[۳]. با ارائه اولین استاندارد مدیریت امنیت اطلاعات در سال ۱۹۹۵، نگرش سیستماتیک به مقوله ایمن‌سازی فضای تبادل اطلاعات شکل گرفت. براساس این نگرش، تامین امنیت فضای تبادل اطلاعات سازمان‌ها بصورت مداوم و در یک چرخه ایمن‌سازی شامل طراحی، اجرا، ارزیابی و اصلاح[۳] (PDCA) انجام می‌گیرد.

۲.۱. استاندارد مدیریت امنیت اطلاعات

یکی از استانداردهای موجود و شاخص در زمینه مدیریت امنیت اطلاعات، مجموعه ISO/IEC 27000، شامل استانداردهای امنیت اطلاعات است که تحت عنوان خانواده استاندارد ISMS شناخته می‌شود. این مجموعه به طور مشترک توسط سازمان بین‌المللی استاندارد[۴] (ISO) و کمیسیون بین‌المللی الکتروتکنیک[۵] (IEC) منتشر شده است. این مجموعه بهترین توصیه‌ها را بر پایه تجربیات عملی در مدیریت امنیت اطلاعات، مخاطرات و کنترل در کلیه ابعاد سیستم مدیریت امنیت اطلاعات بیان می‌نماید. استاندارد ISO 27001:2005 با عنوان نیازمندی‌های سیستم‌های مدیریت امنیت اطلاعات در سال ۲۰۰۵ تدوین شده است که شامل ٤ مرحله PDCA به معنی طراحی(Plan)، اجرا (Do) ، ارزیابی (Check) و اصلاح (Act) می‌باشد. پیش‌نویس نسخه جدید این استاندارد نیز در سال ۲۰۱۳ ارائه شده است[٤].

۲.۲. استاندارد مدیریت امنیت اطلاعات در حوزه صنعت برق و انرژی

استاندارد ISO/IEC TR 27019:2013، استاندارد مدیریت امنیت اطلاعات در حوزه صنعت برق و انرژی از خانواده ISO/IEC 27k در جولای ۲۰۱۳ توسط ISO و IEC منتشر شده است. این استاندارد دستورالعمل‌هایی را مطابق با استاندارد ISO/IEC 27002 برای مدیریت امنیت اطلاعات در سیستم‌های کنترل فرآیند شرکت‌های انرژی(برق، گاز و حرارت) فراهم می‌آورد. هدف این استاندارد گسترش مجموعه استانداردهای ISO/IEC 27k و پیاده‌سازی سیستم مدیریت امنیت اطلاعات(ISMS) مطابق با الزمات استاندارد ISO/IEC 27001 و گسترش

[2] Information Security Management System

[3] Plan, Do, Check & Act
[4] The International Organization for Standardization
[5] International Electrotechnical Commission

آن از حوزه کسب و کار به حوزه سیستم‌های کنترل فرآیند و اتوماسیون می‌باشد.

استاندارد ISO/IEC TR 27019 ترجمه‌ای از استاندارد ۲۷۰۰۹ موسسه استاندارد آلمان[6] (DIN) است[۵]. حوزه کاری استاندارد ISO/IEC TR 27019:2013، سیستم‌های کنترل فرآیند شرکت‌های فعال در حوزه انرژی برای کنترل و نظارت بر تولید، انتقال، ذخیره و توزیع برق، گاز و حرارت می‌باشد. این محدوده به طور خاص شامل سیستم‌ها، برنامه‌ها و اجزای زیر است[٦]:

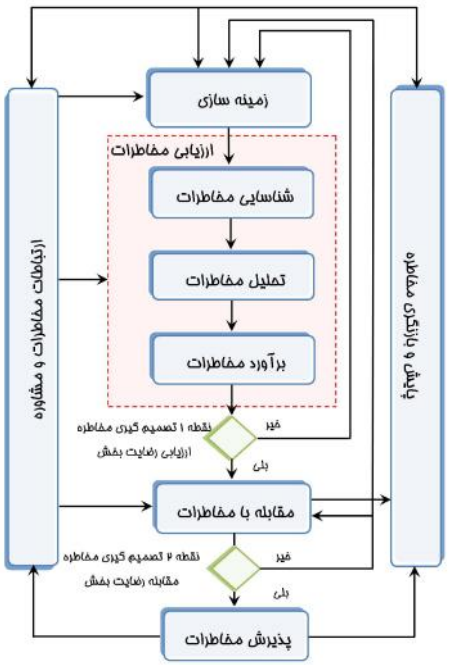
- ✓ مجموعه IT شامل پشتیبانی از نظارت، اتوماسیون و کنترل فرآیند مرکزی و توزیع شده
- ✓ کنترل‌کننده‌های الکترونیکی و اجزای اتوماسیون از قبیل تجهیزات در محل، تجهیزات کنترلی شامل PLC، سنسورهای الکترونیکی و عناصر فعال
- ✓ فن‌آوری‌های ارتباطی در حوزه کنترل فرآیند در شبکه، اندازه‌گیری و کنترل از راه دور
- ✓ تجهیزات اندازه‌گیری تولید یا مصرف انرژی یا اندازه‌گیری میزان آلودگی
- ✓ سیستم‌های حفاظتی و تامین امنیت الکترونیکی همانند رله‌های حفاظتی
- ✓ اجزای توزیع شده در آینده شبکه‌های هوشمند
- ✓ تمامی نرم افزارها، سفت افزارها و برنامه‌های کاربردی نصب شده بر روی سیستم‌های مذکور

۲.۳. مراحل ایجاد سیستم مدیریت امنیت اطلاعات

هر سازمان باید به ایجاد، پیاده‌سازی، اجرا، پایش، بازنگری و نگهداری یک سیستم مدیریت امنیت اطلاعات مستند شده درچارچوب تمامی فعالیت‌های کلان خود و مخاطراتی که با آن روبرو می‌باشد بپردازد. فرآیندها بر پایه مدل PDCA بوده و اغلب خروجی هر فرآیند، ورودی فرآیند بعدی می‌باشد. مدیریت مخاطرات[7] یک فرآیند جامع بمنظور تعیین، شناسایی، کنترل و مقابله با مخاطرات اجرایی برخی فعالیت‌ها و فرآیندها به سطح قابل قبول و کسب تائید مدیریت است. مدیریت مخاطرات با استفاده از مجموع نتایج ارزیابی مخاطرات و مسائل فنی، اقتصادی، اجتماعی و سیاسی، مکانیزمی را جهت تصمیم‌گیری در مورد نیاز به کاهش مخاطره یا روش‌های کاهش مخاطره فراهم می‌نماید. در جدول ۱ خلاصه فعالیت‌های مدیریت مخاطرات امنیت اطلاعات در چهار مرحله فرآیندهای ISMS نشان داده شده است. مرحله طرح‌ریزی سیستم مدیریت مخاطرات امنیت اطلاعات شامل مراحل زمینه‌سازی، ارزیابی مخاطرات[8]، تدوین برنامه مقابله با مخاطرات[9] و پذیرش مخاطرات می‌باشد[۷].در شکل ۱ چرخه‌کاری فرآیند مدیریت مخاطرات براساس استاندارد ISO/IEC 27005:2011 نشان داده شده است.

جدول ۱: هم راستایی ISMS و مدیریت مخاطرات امنیت اطلاعات

فرآیند ISMS	*فرآیند مدیریت مخاطرات امنیت اطلاعات*
طرح ریزی (PLAN)	زمینه سازی ارزیابی مخاطرات تدوین برنامه مقابله با مخاطرات پذیرش مخاطرات
انجام(Do)	پیاده‌سازی برنامه مقابله با مخاطرات
بررسی(Check)	پایش و بازنگری مستمر مخاطرات
اصلاح(Act)	نگهداری و بهبود فرآیند مدیریت مخاطرات



شکل ۱: فرآیند مدیریت مخاطرات امنیت اطلاعات[۷]

[6] Deutsches Institut für Normung
[7] Risk Management
[8] Risk Assessment
[9] Risk Treatment Plan

۳.سرویس‌های امنیتی

امنیت اطلاعات یعنی حفظ محرمانگی[10]، تمامیت[11] و دسترس‌پذیری[12] اطلاعات. علاوه بر این مفاهیم سه‌گانه می‌توان مفاهیم دیگری از قبیل احراز اصالت[13]، مجازشناسی[14] و عدم انکار[15] در نظر گرفت[۳]. به این مفاهیم شش‌گانه، سرویس‌های امنیتی[16] گفته می‌شود که تضمین‌کننده امنیت با استفاده از مکانیزم‌های امنیتی[17] است. مکانیزم‌های امنیتی نیز روش‌های تشخیص، جلوگیری و بازیابی از حملات می‌باشد. هر مکانیزم امنیتی نیز در واقع یکی از روش‌های پیاده‌سازی یک سیاست امنیتی است که تعیین می‌کند که از نظر امنیتی چه فعالیت‌هایی مجاز و یا غیرمجاز است. این که یک سازمان از چه سیاست امنیتی استفاده کند بستگی به میزان امنیت مورد نیاز و بودجه آن دارد. در جدول ۲ نمونه راهکارها و کنترل‌ها جهت تامین سرویس‌های امنیتی در یک سیستم اطلاعاتی نشان داده شده است.

جدول ۲: راهکارها و کنترل‌های تامین سرویس‌های امنیتی

سرویس‌های امنیتی	*راهکارها و کنترل‌های امنیتی*
محرمانگی	رمزنگاری، ایجاد ترافیک مجازی
تمامیت	کد احراز اصالت پیام، امضای دیجیتال و توابع چکیده‌ساز
دسترس‌پذیری	طرح تداوم فعالیت شبکه، سیستم‌های پشتیبانی، ظرفیت‌دهی کافی به سیستم
احراز اصالت	گذرواژه، دستگاه رمزیاب، کارت‌های هوشمند، تکنیک‌های بیومتریک، الگوریتم کلید عمومی
مجاز شناسی	کنترل دسترسی، امضای دیجیتال
عدم انکار	امضای دیجیتال

٤.تهدیدات امنیتی

تهدید عاملی است که به طور بالقوه می‌تواند باعث صدمه به سازمان یا سیستم‌های فن‌آوری اطلاعات، شبکه و ... گردد. با توجه به گستردگی تهدیدات امنیتی، این مقاله معطوف به تهدیدات امنیتی در فن‌آوری اطلاعات و شبکه‌های رایانه‌ای می‌باشد. در شبکه‌های رایانه‌ای هر گونه تلاش برای از بین‌بردن، افشا، تغییر، غیرفعال کردن، سرقت یا به دست آوردن دسترسی‌های غیرمجاز یا استفاده غیرمجاز از یک دارایی حمله گفته می‌شود[۸]. امروزه برخلاف گذشته تدارک حملات با در اختیار داشتن ابزارهای فراوان و در دسترس، به دانش زیادی احتیاج ندارند و تعداد حملات علیه امنیت اطلاعات به طور قابل ملاحظه‌ای افزایش یافته است. برای برآورد میزان امنیت، باید فرض نمود که مهاجم به اطلاعات ارسالی از طریق کانال مخابراتی و تمام جزئیات مربوط به تابع رمزنگاری بجز بیت‌های کلید کاملا دسترسی دارد. مطابق با اصل کرشهف، تنها مخفی بودن کلید رمز است که امنیت را تامین می‌کند. حملات در یک شبکه رایانه‌ای، حاصل پیوند سه عنصر مهم سرویس‌های فعال، پروتکل‌های استفاده شده و پورت‌های باز می‌باشد. کارشناسان امنیت اطلاعات باید با تمرکز بر سه محور فوق، شبکه‌ای امن و مقاوم در مقابل انواع حملات را ایجاد و نگهداری نمایند.

حملات در شبکه‌های رایانه از نظر تاثیر به دو دسته فعال و غیرفعال تقسیم می‌شوند. حملات فعال[18]، سیستم یا شبکه را تغییر می‌دهند، ولی حملات غیرفعال[19] به دنبال جمع‌آوری اطلاعات از سیستم‌ها هستند. حملات فعال، بر روی دسترس‌پذیری، تمامیت و صحت داده‌ها موثر هستند، در حالیکه حملات غیرفعال، محرمانگی را مختل می‌نمایند. برای مثال حملات منع سرویس توزیع شده[20](DDos)، حمله بازپخش[21]، حملات با استفاده از بدافزارهایی از قبیل تروجان‌ها، ویروس‌ها، کرم‌های رایانه‌ی جزو حملات فعال و حملاتی همانند مرد در میانه[22](MITM)، تجزیه و تحلیل ترافیک شبکه، حملات با استفاده از بدافزارهایی از قبیل جاسوس‌افزارها و کلیدخوان‌ها[23] جزو حملات غیرفعال می‌باشند.

۵.راهکارها و کنترل‌های امنیتی در فراسامانه هوشمند اندازه‌گیری و مدیریت انرژی (فهام)

حوادث رایانه‌ای می‌توانند خسارات زیادی را به سازمان‌هایی که از بستر فناوری اطلاعات استفاده می‌کنند، وارد نمایند. یک حادثه رایانه‌ای گسترده می‌تواند با تحت تاثیر قرار دادن یک یا چند سازمان و نهاد در داخل کشور، مشکلات مختلفی را برای کشور ایجاد کند. شرایط خاص کشور باعث شده است تا هر روز تهدیدات امنیتی جدیدی برای ایجاد اختلال در بستر فن‌آوری اطلاعات یا دسترسی به داده‌های سازمان‌ها و نهادها صورت

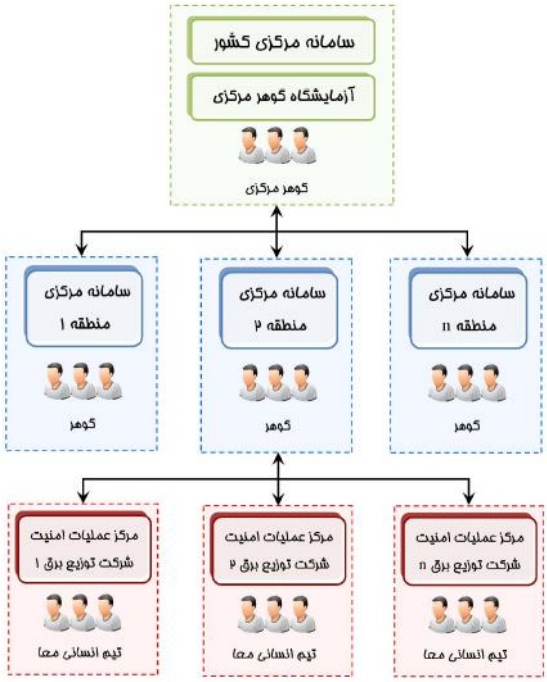
[10] Confidentiality or Privacy
[11] Integrity
[12] Availability
[13] Authentication
[14] Authorization
[15] Non-Repudiation
[16] Security Services
[17] Security Mechanisms

[18] Active Attacks
[19] Passive Attacks
[20] Distributed Denial of Service Attack
[21] Replay Attack
[22] Man in The Middle
[23] Key Logger

گیرد. به همین خاطر حائز اهمیت است که از راهکارهای مناسب برای پایش و شناسایی به موقع تهدیدات امنیتی ایجاد شده و مدیریت آن‌ها استفاده گردد. در ادامه به معرفی چندین راهکار امنیتی پیشنهادی در سیستم‌های اطلاعاتی طرح فهام پرداخته شده است.

۵.۱. گوهر و مرکز عملیات امنیت

مشابه دیگر سامانه‌های جهان، تامین امنیت فراسامانه هوشمند اندازه‌گیری و مدیریت انرژی ایران از طریق استقرار سامانه مرکز عملیات امنیت و مقابله با بدافزار و گروه واکنش هماهنگ رخداد(گوهر) میسر خواهد بود. در فرآیند اجرایی طرح فهام، کشور به چند ناحیه تقسیم شده است. در هر ناحیه یک سامانه مرکزی و گوهر منطقه‌ای مستقر بوده و در سطح کشور نیز به منظور هماهنگی و تبادل دانش بین آنها، یک سامانه مرکزی کشوری و گوهر مرکزی پیش‌بینی شده است. همچنین برای هر یک از شرکت‌های توزیع زیر مجموعه یک ناحیه نیز یک مرکز عملیات امنیت[۲۴] (SOC) در نظر گرفته شده است. در شکل ۲ ساختار سلسله مراتبی مراکز عملیات امنیت و گوهرهای منطقه‌ای و مرکزی نشان داده است.



شکل ۲ ساختار سلسله مراتبی مراکز عملیات امنیت

هر گوهر در سه دسته پاسخ‌گویی، پیش‌گیری و بهبود، خدمات خود را ارائه می‌دهد. خدمات این گروه شامل خدمات رسیدگی به حادثه، رسیدگی به آسیب‌پذیری، رسیدگی به بدافزار، تحلیل مخاطره، تداوم فعالیت، ارزیابی، پیکربندی ابزارها و مشاوره امنیتی می‌باشد. گوهر مرکزی نیز علاوه بر سرویس‌های گوهر، باید قادر به ارائه سرویس‌های تحلیل و هماهنگی در رسیدگی به حادثه، آسیب‌پذیری و بدافزار و صدور اخطار و هشدار باشد. گوهر مرکزی جهت تحلیل و ارزیابی‌های پیچیده‌تر نیازمند یک آزمایشگاه می‌باشد. همچنین سامانه مرکزی با آزمایشگاه تحلیل بدافزار توانیر و دیگر آزمایشگاه های بدافزار فعال کشور در ارتباط می‌باشد.

مرکز عملیات امنیت، مجموعه‌ای از سامانه‌های نرم‌افزاری و تیم‌های انسانی است که مسئولیت تشخیص حوادث با دریافت و پردازش رخدادنما و هشدارها از پایین‌ترین منابع شبکه تحت پایش خود و همچنین اجرای فرآیندهای از پیش تعیین شده به منظور مقابله با حوادث را بر عهده دارد. سامانه رسیدگی به حوادث با مرکز عملیات امنیت در ارتباط بوده و دستورات لازم برای رسیدگی به حوادث را از طریق تیم انسانی مرکز عملیات امنیت(معا) و یا با استفاده از فرامین از پیش تعیین شده، برای اجزا شبکه فهام ارسال می‌نماید. مرکز عملیات امنیت، شامل سامانه‌های گردآوری و ثبت، تحلیل، رسیدگی به حوادث، ارسال دستورات، پایگاه دانش، مدیریت و نگهداری، آرشیو و کنسول می‌باشد.

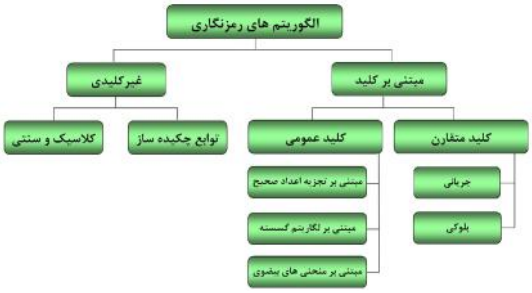
۵.۲. رمزنگاری

رمزنگاری[۲۵] دانشی است که به بررسی و شناخت اصول و روش‌های انتقال یا ذخیره اطلاعات به صورت امن می‌پردازد، در حالیکه ممکن است کانال‌های ارتباطی یا محل ذخیره اطلاعات نیز ناامن باشد. مطابق با شکل ۳، طبقه‌بندی الگوریتم‌های رمزنگاری به دودسته مبتنی بر کلید و غیرکلیدی تقسیم می‌شوند. الگوریتم‌های غیرکلیدی شامل توابع درهم‌سازی و روش‌های رمزنگاری کلاسیک و سنتی می‌باشند. الگوریتم‌های رمزنگاری مبتنی بر کلید نیز به دو دسته الگوریتم‌های کلید متقارن[۲۶] و کلید عمومی[۲۷] تقسیم‌بندی می‌گردد. در الگوریتم کلید متقارن، کلید رمزگذاری و رمزگشایی یکسان بوده و تنها در اختیار فرستنده و گیرنده قرار دارد و برای تبادل آنها نیاز به یک کانال امن می‌باشد. در الگوریتم کلید عمومی، کلید رمزگذاری و رمزگشایی متفاوت بوده و دارای یک کلید عمومی و یک کلید خصوصی است که نیاز به کانال امن برای مبادله کلید ندارد. همچنین از نظر محاسباتی بدست آوردن یکی با دانستن دیگری غیرممکن است.

[24] Security Operations Center

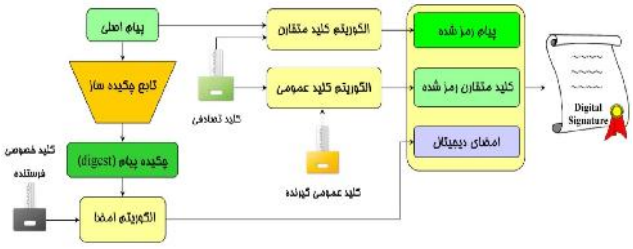
[25] Cryptography
[26] Symmetric Key Encryption
[27] Public Key Encryption

الگوریتم‌های کلید عمومی هم برای عمل رمزنگاری و هم امضا دیجیتال به کار گرفته شده و سرعت کمتری نسبت به الگوریتم‌های متقارن دارا می‌باشند. روش مناسب ترکیبی، استفاده از الگوریتم‌های کلید متقارن برای رمز نمودن پیام اصلی[۲۸] و الگوریتم کلید عمومی برای تبادل کلید رمزنگاری الگوریتم‌های متقارن است. امنیت سیستم‌های رمزنگاری وابسته به دو عامل اساسی قدرت الگوریتم و طول کلید است. با فرض اینکه در قدرت الگوریتم هیچ خللی وارد نمی‌شود، راهی برای شکستن آن غیر از حمله جستجوی فراگیر[۲۹] وجود ندارد.



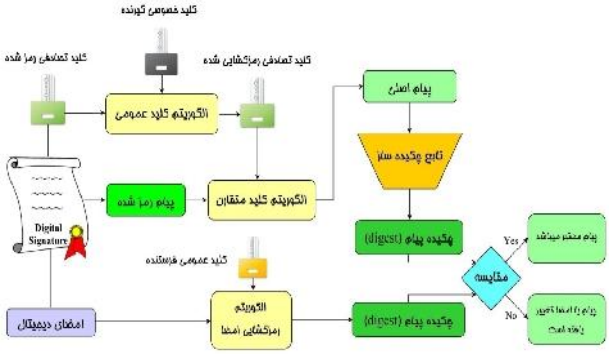
شکل ۳: طبقه‌بندی الگوریتم‌های رمزنگاری[۲]

جهت تامین چهار سرویس امنیتی محرمانگی، تمامیت، احراز اصالت و انکار ناپذیری می‌توان از کامل‌ترین روش یعنی استفاده از سه الگوریتم کلید عمومی، کلید متقارن و امضای دیجیتالی استفاده نمود. در سند الزامات طرح فهام استفاده از الگوریتم کلید عمومی ECC با طول کلید ۲۵٦ یا RSA با طول کلید ۱۰۲٤ و الگوریتم کلید متقارن AES با طول کلید ۱۲۸ اشاره شده است[۱۰]. شکل ٤ فرآیند الحاق امضای دیجیتال به پیام رمزشده با الگوریتم متقارن و رمزگذاری کلید متقارن با استفاده از الگوریتم کلید عمومی در فرستنده را نشان می‌دهد. در شکل ۵ نیز عکس این عمل شامل فرآیند تایید اعتبار پیام با امضای دیجیتالی، رمزگشایی کلید الگوریتم متقارن با استفاده از کلید خصوصی گیرنده و سپس باز نمودن پیام رمزشده با کلید مذکور انجام می‌گردد.



شکل ٤: الحاق امضای دیجیتال به پیام رمز[۲]

[28] Plain Text
[29] Brute Force Attack



شکل ۵: تایید اعتبار پیام با امضای دیجیتالی و رمزگشایی پیام رمز شده[۲]

در این دو شکل کلید تصادفی متقارن با رنگ سبز، کلید عمومی با رنگ زرد و کلید خصوصی با رنگ مشکی نشان داده شده است. مراحل فرآیند رمزنگاری و رمزگشایی در این روش به شرح زیر می‌باشد[۲]:

۱) رمزگذاری پیام اصلی با استفاده از یک کلید تصادفی(کلید متقارن)

۲) رمزگذاری کلید تصادفی مرحله قبل با استفاده از کلید عمومی گیرنده

۳) تولید چکیده پیام اصلی و تولید امضای دیجیتالی

٤) رمزگذاری امضای دیجیتالی با استفاده از کلید خصوصی فرستنده

۵) تلفیق کلید تصادفی رمزشده و پیام رمزشده با امضای دیجیتالی

٦) ارسال بسته توسط شبکه به گیرنده

۷) جداسازی محتوای رمزشده شامل پیام اصلی، کلید تصادفی و امضای دیجیتالی از یکدیگر پس از دریافت

۸) رمزگشایی کلید تصادفی رمزشده با استفاده از کلید خصوصی گیرنده

۹) رمزگشایی پیام اصلی با استفاده از کلید تصادفی بدست آمده در مرحله قبل

۱۰) تولید چکیده از پیام اصلی بدست آمده از مرحله قبل

۱۱) رمزگشایی امضا با استفاده از کلید عمومی فرستنده

۱۲) مقایسه چکیده پیام محاسبه شده و چکیده پیام بدست آمده از امضا به منظور اعتبار سنجی

۵.۳. سیستم مدیریت کلید

یک سیستم مدیریت کلید[۳۰](KMS) شامل سیاست‌ها، فرآیندها و اجزا (سخت‌افزار، نرم‌افزار و سفت‌افزار) و تجهیزاتی است که برای تولید،

[30] Key Management System

توزیع، ذخیره، حفاظت و انهدام کلیدهای رمزنگاری به کار گرفته می‌شوند. مدیریت کلید شامل عملیات تولید، توزیع و نگهداری کلید می‌باشد. بهترین روش برای تولید کلید به صورت تصادفی، استفاده از مولدهای اعداد شبه تصادفی است. برای توزیع کلید نیز می‌توان از الگوریتم‌های کلید عمومی به همراه امضای دیجیتال بهره برد که می‌توان به الگوریتم‌های رمزنگاری منحنی بیضوی[۳۱] (ECC) و الگوریتم تبادل کلید دیفی–هلمن[۳۲](DH) اشاره نمود. برای احراز اصالت در تبادل کلید نیز چندین پروتکل از قبیل احراز اصالت براساس کلید مشترک و مخفی، احراز اصالت با استفاده از الگوریتم کلید عمومی، احراز اصالت توسط مرکز توزیع کلید[۳۳](KDC)، احراز اصالت با طرح توزیع کلید کربروس[۳۴] وجود دارد، در سیستم‌های اندازه‌گیری هوشمند دو مورد اول کاربردی‌تر می‌باشند. چهار قاعده کلی که باید جهت طراحی یک پروتکل احراز اصالت در نظر گرفته شود به شرح زیر است :

۱) یک شروع‌کننده باید قبل از پاسخ دهنده هویت خود را احراز نماید، در غیر این صورت نفوذگر بدون احراز اصالت می‌تواند اطلاعات با ارزشی از پاسخ دهنده را بدست آورد.

۲) شروع‌کننده و پاسخ‌دهنده باید از کلیدهای متفاوتی برای احراز خود استفاده نمایند، حتی اگر به معنای تعریف دو کلید مشترک و مستقل باشد.

۳) شروع‌کننده و پاسخ‌دهنده باید رشته‌های چالش خود را که به آن نانس[۳۵] گفته می‌شود از مجموعه‌های متفاوتی انتخاب نمایند.

٤) پروتکل باید در مقابل حملاتی که در اثر نشست‌های موازی همزمان امکان‌پذیر می‌گردد مقاوم بوده و اطلاعات یک نشست نباید در نشست دیگر قابل استفاده باشد.

نگهداری کلید نیز شامل عملیات بروزرسانی، ذخیره و پشتیبان‌گیری از کلید است. ذخیره کلید باید با استفاده از کمک پردازنده‌های امن رمزنگاری[۳٦]، ماژول بستر معتمد[۳۷](TPM) و یا ماژول امنیت سخت‌افزاری[۳۸](HSM) صورت گیرد تا امکان دسترسی آسان به آنها در کنتورها و دیگر تجهیزات شبکه وجود نداشته باشد که در حال حاضر نحوه پیاده‌سازی سخت‌افزاری آن در طرح فهام در حال مطالعه و بررسی می‌باشد.

[31] Elliptic Curve Cryptography
[32] Diffie–Hellman Key Exchange
[33] Key Distribution Center
[34] Kerberos Key Distribution Scheme
[35] Nonce
[36] Secure Cryptogrphic Coproccessor
[37] Trusted Platform Module
[38] Hard Security Module

٦.نتیجه‌گیری

در این مقاله به مباحث پیرامون امنیت اطلاعات در سیستم‌های اندازه‌گیری هوشمند، تهدیدات، سرویس‌ها و نمونه مکانیزم‌های امنیتی و به طور خاص راهکارها و کنترل‌های امنیتی در طرح فهام ایران پرداخته شد. هر سیستم اطلاعاتی برای مقابله با مخاطرات و تامین امنیت اطلاعات خود، نیازمند یک ساختار مدیریت اطلاعات منسجم با مکانیزم امنیتی مناسب است. راهکارها و کنترل‌های استفاده شده در طرح فهام براساس استانداردهای معتبر بین‌المللی است که در پروژه‌های بزرگ و مطرح دنیا به کار گرفته شده‌اند و از نظر امنیتی نیز در سطوح قابل قبولی می‌باشند. این مکانیزم‌ها می‌توانند با تداوم فعالیت شبکه و کاهش تهدیدات امنیتی و اثرات آنها، امنیت اطلاعات را تضمین نموده و رضایت‌مندی مشترکین از تداوم سرویس را افزایش دهند.

منابع

[1] M. E. Whiteman & H. J. Maltord, “Information Security: An Introduction,” Principles of Information Security, 4th ed. Boston, MA, Course Technology, 2012, pp. 3-7.

[2] M. Rezaeian,H. Modaghegh & N. Salek Gilani, “Information Security in Smart Metering Systems,” *Iran Energy Efficieny Organization(IEEO)*, Department of Smart Metering Systems & Smart Grid, Special Reports, No. 12, Aug. 2013.

[3] *Information Technology -Security Techniques -Information Security Management Systems -Requirements*, ISO/IEC 27001:2005, Oct.2005.

[4] *Information Security Standards* [Online]. Available: http://www.iso27001security.com/html/others.html.

[5] St. Beirer. (2013, Jul 22). *ISO/IEC TR 27019 for Energy Utilities Published*, [Online] Available: http://www.digitalbond.com/blog/2013/07/22/isoiec-tr-27019-for-energy-utilities-published/.

[6] *Information Security Management Guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry*, ISO/IEC TR 27019:2013, Jul.2013

[7] *Information Technology - Security Techniques - Information Security Risk Management*, ISO/IEC 27005:2011, 2011..

[8] *Information technology - Security techniques - Information security management systems - Overview and vocabulary*, ISO/IEC 27000:2009, May.2009.

[۹] واژه‌نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات(افتا) ، گروه واژه‌گزینی انجمن رمز ایران، نشر دانشگاه صنعتی شریف، چاپ اول، ۲۲۸ ص، سال ۱۳۹۰.

[10] “General, Economic, Functional, Technical & Communications Requirements of Iranian Smart Metering Project (FAHAM),” *Iran Energy Efficieny Organization(IEEO)*, Department of Smart Metering Systems & Smart Grid, Final Rep, Dec. 2011