کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی
بین المللی و
ترفند های جستجو

کارگاه آنلاین
روش تحقیق و مقاله نویسی علوم انسانی

کارگاه آنلاین
پرپوزال نویسی و پایان نامه نویسی

نقد و بررسی استاندارد امنیتی IEC 62351

پدیده نوبخت [۱و۲]، امیر مسعود امینیان مدرس [۲]

۱ – شرکت برق منطقه ای خراسان
مشهد، ایران
p.nobakht@krec.ir

۲ – دانشگاه صنعتی سجاد
مشهد، ایران
aminian.mod@gmail.com

چکیده — به دلیل وجود تفاوتهای محسوس بین سیستمهای مخابرات صنعتی با سیستمهای اداری، بازرگانی و جدید بودن سیستمهای اتوماسیون پست، نمیتوان از امکانات امنیتی موجود برای اتوماسیون پستها استفاده کرد . عملکرد سیستمهای قدرت چالشهای امنیتی بسیار زیاد و متفاوتی با سایر صنایع دارد. اکثر اقدامات امنیتی تدبیر شده برای پیشگیری از حمله مهاجمین اینترنتی است. از طرفی محیط اینترنت بسیار متفاوت با محیط عملکردی سیستمهای قدرت است. بنابراین صنعت دارای کمبود دانش در زمینه الزامات امنیتی و تاثیرات بالقوه اقدامات امنیتی در عملکرد سیستمهای قدرت میباشد. سرویسها و تکنولوژیهای امنیتی توسعه یافته دارای تفاوتهای اساسی نسبت به الزامات مورد نیاز شبکه قدرت مانند جلوگیری از انکار و استفاده از باند باریک هستند. بنابراین باید استانداردهای خاص این شبکه توسعه یابد. در این مقاله استاندارد های امنیتی تدوین شده برای شبکه های هوشمند معرفی شده و یکی از اساسی ترین استانداردها مورد نقد و بررسی قرار می گیرد.

واژه‌های کلیدی — استاندارد؛ شبکه هوشمند؛امنیت؛ IEC TC57؛ IEC 62351

۱.مقدمه

شبکههای هوشمند، تحت تاثیر حملات فیزیکی هستند ، که از ترکیب عملکرد تجهیزات سیستم قدرت با تجهیزات کنترل تشکیل شده است. این سیستمها دارای قابلیت توسعه، حفاظت و کار در زمان قطع ارتباط یا کار در شرایط غیرعادی است. به دلیل نیاز تامین برق پایدار باید سیستمهای هوشمند توانایی برگشت به کار پس از حمله را داشته باشند و نیاز است بسیار سریع به مدار برگردند. در نهایت باید امکان حفاظت وپیگیریهای قانونی حملات توسط ثبت زمان و وقایع فراهم گردد. بنابراین امنیت سایبری برای این سیستم ها بسیار شبیه سیستمهایی است که باید از حمله سایبری به آنها جلوگیری گردد. امنیت شامل محدوده بسیار فراتر از تصدیق کاربران و رمز نگاری پروتکلهای ارتباطی است. برای ایجاد امنیت باید به سیاستهای امنیتی، مکانیزمهای کنترل دسترسی، مدیریت کلید رمزنگاری، ارزیابی ثبت وقایع و سایر زیر بناهای حفاظتی توجه داشت. امنیت باید از ابتدا در سیستمها برنامهریزی و طراحی گردد. چنانچه از ابتدا برنامهریزی امنیتی در نظر گرفته نشود، هنگام بازنگری باید هزینههای پشگیری به روزرسانی گردد. امنیت باید در تمام سطوح ساختار سیستم در نظر گرفته شود. تامین امنیت یک فرآیند است که باید به صورت متناوب و پیوسته تکرار شود. امنیت باید بر اساس سیاستهای زیربنایی سازمان و تهدیدها به روز رسانی گردد. در بخشهای بعدی استانداردهایی که برای امنیت شبکه - های هوشمند معرفی شدهاند ارائه خواهند شد. نکته مهم این مقاله اینست که یکی از مهمترین استانداردهای امنیتی شبکهای هوشمند که IEC 62351 نام دارد با جزئیات بیشتر معرفی شده و مشکلات اساسی و اجرایی آن مطرح خواهد شد.

۲.استانداردهای امنیتی

برای شبکههای هوشمند استانداردهای امنیتی تعریف شده است که این استاندارد ها به شرح ذیل دستهبندی میشوند:

۲.۱. استانداردهای عمومی امنیت

استاندارد CC: این استاندارد مربوط به تجهیزات و کاربردهای تصدیق، مانند دیوار آتش است. تلاش این استاندارد ارزیابی و تصدیق اختیارات کاربران در کنترل بخش هایی از EALs است.

1 - Common Criteria
2 - evaluation assurance levels

استاندارد ISO/IEC 17799: این استاندارد مربوط به فرآیندهای داخلی شرکت و کنترلهایی که در محدودههای متفاوت دهگانه(مانند برنامه - ریزی استمرار کسب و کار، کنترل دسترسی سیستم، امنیت فیزیکی، مدیریت اپراتور ها، کامپیوتر ها و سیاست های امنیتی)می باشد.

۲.۲. استانداردهای امنیتی سیستمهای صنعتی

استاندارد IEEE 1402 : استاندارد امنیتی پستها است که بیشتر به امنیت فیزیکی میپردازد.

استاندارد PCSRF[3]: با هدف جمعآوری الزامات استاندارد برای تهیه سیستمهای کنترل صنعتی جدید بنیانگذاری شده است.

استاندارد ISA SP99 : برای امنیت سیستمهای کنترل کارخانهای استفاده میشود و مستندات و راهنماییهایی در رابطه با امنیت IT در سیستمهای اتوماسیون و کنترل صنعتی ارائه کرده است. این استاندارد سختافزار و نرمافزار سیستمهایی مانند DCS[4]، SCADA[5]، PLC و سیستمهای تشخیص و نظارت را نیز پوشش می دهد.

استاندارد AGA 12[6] : استاندارد برای امنیت مخابرات SCADA است و ریسکهای مجاور سیستم اسکادا است و به طور خاص به رمزنگاری میپردازد.

استاندارد IEC TC65 : کمیته فنی IEC که برای صدور استانداردهای مرتبط با گذرگاهها و سایر شبکههای مخابرات دیجیتال تشکیل شده است. کمیته فنی 65 A برای صدور استانداردهای امنیتی سیستم کنترل و اندازه - گیری فرآیندهای IEC 61850 از سال ۲۰۰۳ شروع به فعالیت کرده است.

استاندارد NERC 1200[7] : برای مستندسازی ایجاد و پشتیبانی حدود ۱۶ بعد مختلف امنیت IT مانند کنترل دسترسی، امنیت فیزیکی، پشتیبانی رویداد ها، سیاست ها و آموزشها تعریف شده است.

استاندارد FDA[8] : شامل جزئیات ممیزی و نظارت کارخانهای و تولید و نگهداری تجهیزات الکتریکی است.

استاندارد IAONA[9] : راهنمای امنیتی برای شبکه های اترنت صنعتی می باشد. تمرکز این استاندارد روی سرویس های TCP/UDP/IP است و به شناسایی نقاط ضعف امنیتی است.

3 - Process Control Security Requirements Forum
4 - distributed control systems
5 - supervisory control and data Acquisition
6 - American Gas Association
7 - North American Electric Reliability Council
8 - Food and Drug Administration
9 - Industrial Automation Open Networking Alliance

استاندارد CIGRE[10] : شامل امنیت سیستمهای اطلاعاتی و اینترانت سیستمهای قدرت است.

۲.۳. امنیت پروتکلهای اتوماسیون صنعتی در سطح LAN[11]/WAN[12]

برای پروتکلهای مخابرات صنعتی برخی استانداردهای امنیتی مشترک به شرح ذیل تعریف شده است:

استاندارد OPC[13] : مشابه مدل COM[14] مایکرو سافت است. مشخصه OPC DA[15] برای انتقال به موقع دادههای پردازش شده از مهر زمان و وضعیت اطلاعات تجهیزات اتوماسیون(مانند کنترلکننده های سطوح بالاتر) استفاده کرده است.

استاندارد MMS[16]: استاندارد لایه کاربردی و برای پیامهای مخابراتی ارسالی از تجهیزات داخل سایت یا PLC ها در محیطهای تولید یکپارچه کامپیوتری است. این استاندارد فقط برای سرویسهای عمومی استفاده می - شود. امروزه MMS به صورت خاص برای استاندارد IEC 61850 مورد استفاده قرار میگیرد. این استاندارد از سال ۱۹۸۰ شناسایی شده است ومخابرات سرور/ مشتری و نقطه به نقطه[17] در سطح شبکه را پوشش می - دهد. لازم به ذکر است که قابلیت اعتماد و عدم انکار توسط MMS تامین نخواهد شد.

استاندارد IEC 61850: این استاندارد جهت تعیین وجود نرم افزار، مدل داده، سرویسها، پروتکلها و قالب دادهها برای اتوماسیون پستهای شبکه قدرت مورد استفاده قرار می گیرد. استاندارد IEC 61850 تصدیق نقاط، تصدیق کاربران و کنترل دسترسی سیستم را تصریح کرده است. برای شروع ارتباط، مشتری باید پارامترهای تصدیق(کلمه عبور+ شناسه کاربر+ منظور) را برای سرور ارسال نماید. کلیه فعالیتهای کنترلی اپراتور باید قبل از اخذ مجوز بررسی و سپس مجوزهای مورد نیاز صادر گردد. استاندارد IEC 61850 به MMS نگاشت شده است. استاندارد امنیتی موجود از لایه اترنت پشتیبانی نمی کند و هیچ ابزار امنیتی برای انتقال داده GES[18] و SMS[19] ندارد. گیرندهها دادههای با آدرس MAC را شناسایی می کنند اما

10 - International Council on Large Electric Systems
11 - Local Area Network
12 - Wide Area Network
13 - Open Process Control
14 - component object model
15 - OPC data access
16 - Manufacturing Messaging Specification
17 - peer-to-peer
18 - generic substation events
19 - sampled measured values

به دلیل جعل ساده آدرسهای MAC ، تصدیق ایجاد شده به لحاظ امنیتی ضعیف است.

استاندارد ICCP[20]: این استاندارد برای ارتباط گسترده بین مراکز شبکه انتقال مانند مراکز کنترل و پست های فوق توزیع و انتقال میباشد. حدود وظایف این استاندارد مشابه OPC است. در اصل این استاندارد یک استاندارد امنیتی نیست اما توسط گروه امنیت IEC منتشر شده است و در رابطه با آسیبپذیری و اقدام متقابل سیستم های ICCP به صورت جزئی بحث کرده است.

در نهایت تمرکز اصلی استانداردهای امنیتی مطابق جدول ۱ میباشد.

جدول 1تمرکز اصلی استاندارد های امنیتی [2]

نام استاندارد	تمرکز اصلی
NIST SGIP-CSWG	شبکه هوشمند – حملات سایبری
NERC CIP	مقررات حملات سایبری تجهیزات قدرت آمریکای شمالی
IEC 62351	امنیت داده و امنیت در مخابرات
IEEE PSRC/H13 & SUB/C10	الزامات امنیت سایبری برای اتوماسیون پستها، سیستمهای کنترل و حفاظت
IEEE 1686	استاندارد برای امنیت سایبری تجهیزات هوشمند الکترونیکی پستها
ISA S99	اتوماسیون صنعتی و امنیت سیستم کنترل

۳.معرفی IEC TC57 WG15

در سال ۱۹۹۷ ضرورت امنیت در پروتکلها مطرح شد و در سال ۱۹۹۹کمیته IEC TC57 WG15 تشکیل شده است. وظیفه این کمیته توسعه استانداردهای امنیتی پروتکلهای ارتباطی تعریف شده در IEC TC57 و نظارت بر ثبت گزارشات تخصصی نشریه های امنیتی است.

مسئولیت توسعه استانداردهای امنیت پروتکلهای ارتباطی خصوصا IEC 60870-5,6، IEC 61850، IEC 61968 و IEC 61970 به عهده IEC TC57 میباشد. به دلیل استناد استانداردهای ارتباطی در لایههای متفاوت به استانداردهای اساسی، یک ارتباط یک به یک بین استاندارد امنیتی IEC 62351 واستاندارد ارتباطی که توسط کمیته IEC TC57 تدوین شده است، وجود ندارد. محدوده کار IEC TC57 آماده کردن استانداردهای جهانی برای تجهیزات کنترل سیستمهای قدرت، سیستمهای مدیریت انرژی، اسکادا، اتوماسیون توزیع، کنترل از راه دور و مبادله اطلاعات زمان واقعی یا زمان غیر واقعی برای برنامه ریزی، اجرا و نگهداری سیستم های قدرت است.

همچنین IEC TC57 پنج استاندارد ارتباطی IEC 60870-5-101, 104, DNP3، IEC 61850، IEC60870-6 IEC 61968, 61970(CIM) و IEC61334 (DLMS) را پوشش می دهد.

این استاندارد شامل ۱۱ فصل است. ارتباط بین IEC 62351 و تهدیدها، حملات و اقدامات امنیتی مطابق جدول ۲ میباشد.

جدول ۲ ارتباط بین IEC 62351 و تهدیدها، حملات و اقدامات امنیتی[3]

Correspondence between IEC 62351 parts and security threats, attacks and measure				
IEC623 51parts	Threats countered	Attacks countered	Security measured	OSI layers
3 - Profiles that include TCP/IP	• Unauthorized access • Unauthorized modification of data • Theft of data	• Eavesdropping through encryption • Man-in-the-middle through message authentication • Spoofing • Replay	• Transport Layer Security (TLS) • Certificates	• Transport layers
4 - Profiles that include MMS	• Unauthorized access • Unauthorized modification of data Theft of data	• Man-in-the-middle • Tamper detection • Message integrity • Replay	• MMS security • Assessment use of TLS as specified in part 3	• Application layer • Transport layers
5 - Security for IEC 60870-5	• Unauthorized access	• Spoofing • Replay • Modification • Some denial of service attacks	•Authentication	• Application layer
6 - Security for IEC 61850 profiles	• Unauthorized access	• Man-in-the-middle • Unauthorized modification of data • Unauthorized modification of message • Tamper detection • Replay	• Digital signature for authentication	• Application layer
7- network management and system security	• Unauthorized access • Denial of service	• Inadvertent problems, including equipment failures, mistakes, and natural disasters Deliberate intrusions, including • disgruntled employees, cyber attacks	• Monitoring an control of the information infrastructure	• All layers

فصل سوم این استاندارد شامل تنظیمات و پارامترهایی با امکان استفاده مفید از TLS است. همچنین این فصل راه حلهایی به شرح ذیل ارائه کرده است:

- حفاظت در برابر استراق سمع با استفاده از رمز نگاری TLS
- امنیت حملات با منشاء انسانی[22] با استفاده از پیام تصدیق

20 - Medium Access Control
21 - Inter Center Control Protocol

22 Man-in-the-middle

- پیش گیری از کلاهبرداری توسط گواهی های امنیتی
- جلوگیری ازحمله ارسال مکرر به واسطه رمز نگاری

لازم به ذکر است که TLS برای عدم انکار راهکاری ارائه نکرده است و نیاز به روش دیگری است.

فصل چهارم عمدتا از TLS برای پیکر بندی، اقدامات امنیتی و به صورت خاص برای تصدیق اطلاعات استفاده میکند.

فصل پنجم در رابطه با امنیت پروتکلهای IEC 60870-5 101 102,103 و DNP3 است. این پروتکلها از مدیاهای ارتباطی با نرخ بیت پایین یا از تجهیزات محاسبهگر استفاده میکنند. بنابراین برای ارتباطات سخت یا محاسبات سخت میتوان از TLS استفاده کرد. پیشنهاد استاندارد در رابطه با حل مساله استراق سمع، آنالیز ترافیک وانکار استفاده از رمزنگاری است. این استاندارد برای مکانیزمهای صحیح مدیریت کلید پاسخ مناسبی ارائه نکرده است ودر پهنای باند باریک فقط برای به روز رسانی کلید مناسب است که صرفه اقتصادی ندارد.

فصل ششم در رابطه امنیت پیام GOOSE استاندارد IEC 61850 است. مهم ترین پروتکل استاندارد IEC 61850 پیام GOOSE میباشد که برای حفاظت رله استفاده میشود. ۳ میلی ثانیه زمان نیاز است تا این پیام به کنترل کننده هوشمند منتقل شود. الزام زمانی مذکور سبب می شود که رمز نگاری یا برخی اقدامات امنیتی که نیازمند زمان هستند برای این پروتکل کاربردی نباشد. بنابراین ارائه راهکار برای این پیام ملاحظات خاص خود را دارد.

۴.مشکلات اجرایی در پیاده سازی IEC 62351

استاندارد IEC 62351 که برای تمام پروتکلهای TC 57 مورد استفاده قرار میگیرد، هنوز در حال توسعه است. کل بخش ۶ این استاندارد برای پیاده سازی عملی نیست و به همین دلیل ویرایش دوم این بخش در دست اقدام است. تدوین چند بخش مهم مانند کنترل دسترسی کاربران یا پشتیبانی کلید ها شروع شده است و نیاز به زمان کافی برای نهایی شدن دارد. امروزه چارچوبهای اصلی برای اجرای بخشهای استاندارد IEC 62351 وجود ندارد.همچنین در کلید رمزنگاری مانند کلید خصوصی و گواهی نامهها نیز فقدان وجود دارد. برای به دست آوردن این چارچوب، سازمانها نیاز به اجرای بخش ۹ استاندارد دارند که هنوز این بخش نهایی نشده است. در حال حاضر TC57 WG15روی بخش ۹ کار می کند. اگرچه طرح اولیه این بخش ارائه شده است اما نیاز به بازنگری در الگوریتم ها و روشها دارد.

ایده و اهداف TC57 WG15 برای تامین امنیت پروتکل های TC57، با نظر اجمالی ساده و اولیه است. ولی نگاه عمیق تر به مشکلات نشان می دهد که برای دستیابی به تامین امنیت باید نگاه دقیقتری داشت. همچنین این استاندارد استفاده از الگوریتمهای رمزنگاری را پیشنهاد کرده است که به دلیل طولانی بودن زمان رمزنگاری الزام زمانی شبکههای هوشمند فراهم نمیشود. از طرفی در تمام استانداردها، اجماع مشترک بین اعضایی که با استاندارد کار می کنند ودر بازنگری دخالت دارند، وجود دارد. در اتوماسیون صنعتی تعداد زیادی کاربر با فرهنگهای امنیتی متفاوت وجود دارند. بنابراین امکان رضایت تمام کاربران وجود نخواهد داشت.

مهمترین چالش استاندارد IEC 62351 برای استفاده از رمز نگاری نامتقارن لیست گواهینامههای با اعتبار و بدون اعتبار است. این استاندارد ریز جزئیات فنی گواهینامهها را اعلام می کند ولی در رابطه با مدیریت آنها اظهار نظر شفافی ندارد. کاربر مقید به اخذ گواهینامه می باشد ولی مرجع صدور گواهی مشخص نیست. همچنین نیاز به مرجعی برای اعلام اعتبار گواهینامهها و زمان تمدید آنها و ارائه لیست گواهینامه های ابطال شده و به روز رسانیاین لیست ها است. در این استاندارد مرکز و مدیر مورد تائید برای انجام این الزامات تعریف نشده است.

در نهایت استفاده از الگوریتمهای رمزنگاری مطرح شده در IEC 62351 به دلایل ذیل در شبکههای هوشمند کاربردی نیست:

- تجهیزات نصب شده مانند سیستم های کنترل و نظارت و RTU ها معمولا دارای قدرت محاسباتی پایین هستند. به روز رسانی سخت افزار تجهیزات نصب شده برای تامین افزایش سرعت الگوریتم رمزنگاری ساده نیست.
- جهت تصدیق بسته، این استاندارد استفاده از امضاء دیجیتال با استفاده ازرمز گذاری نامتقارن RSA را برای پیامهای GOOSE و SV را پیشنهاد کرده است. این با قید زمانی محض ۳ میلی ثانیه برای پاسخ پیام GOOSE و نرخ نمونه گیری بالاتر از ۱۲ کیلو-هرتز برای پیام SV سازگار نیست.
- این استاندارد برای تامین تصدیق داده امضاء دیجیتال HASH 256 را معرفی کرده است که بر اساس قدرت پردازشگرهای موجود در پست نیاز به زمانی بیشتر از الزام زمانی سیستمهای تشخیص نفوذ موجود است.

نتایج نشان می دهد که با سخت افزارهای موجود امکان تامین زمان مورد نیاز پیامهای GOOSE و SV وجود ندارد و نیاز تامین سختافزار مورد نیاز الزام زمانی پیام های GOOSE و SV است. بنابراین برای اجرای شروط این الزامات باید سیستمها ارتقاء یابند که نیاز به صرف زمان و هزینه بالایی است و یا اینکه راه حل بهتر برای استانداردها ارائه گردد.

۵.نتیجه‌گیری

با توجه به اینکه در آیندهای نزدیک شبکه هوشمند جایگزین شبکه کنونی خواهد شد، باید کلیه تهدیدها و ریسکهای این شبکهها شناسایی گردد. چنانچه این تهدیدها جدی گرفته نشود شبکه قدرت دچار خطر بزرگی خواهد بود. بنابراین حرکت به سمت شناسایی استانداردهای امنیتی به اندازه پیادهسازی شبکه هوشمند ضروری است. جهت پیادهسازی امنیت در شبکه باید استانداردهای موجود شناسایی و بومی گردد. با توجه به اینکه استانداردهای امنیتی نیاز به بازنگری و اصلاح دارند،پیشنهاد می شود پروژههای تحقیقاتی در رابطه با تدوین استاندارد بومی برای پیاده سازی امنیت شبکههای هوشمند در دستور کار اساتید و مدیران ارشد وزارت نیرو قرار گیرد.

منابع

[1] DACFEY DZUNG, MEMBER, IEEE, MARTIN NAEDELE, THOMAS P. VON HOFF, ANDMARIO CREVATIN, MEMBER, IEEE, PROCEEDINGS OF THE IEEE ,"Security for Industrial Communication System", VOL. 93, NO. 6, JUNE 2005

[2] Cyber security for substation automation systems by ABB, December 2010

[3] IEC TC57 WG15:IEC 62351 Security Standards for the Power System Information Infrastructure، Frances Cleveland,, WG15 Convenor Xanthus Consulting International،ver 14, June, 2012

[4] F. Hohlbaum, P. Schwyter, F. Alvarez ABB Switzerland Ltd. Switzerland ,"Cyber Security requirements and related standards for Substation Automation Systems" ،D2-02 B11, October 19-20, 2011

[5] Frank Hohlbaum, Markus Braendle, Fernando Alvarez ,"Cyber Security Practical considerations for implementing IEC 62351

کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین آشنایی با پایگاه های اطلاعات علمی بین المللی و ترفند های جستجو

کارگاه آنلاین
روش تحقیق و مقاله نویسی علوم انسانی

کارگاه آنلاین
پروپوزال نویسی و پایان نامه نویسی