پروتکل کنترل صنعتی

IEC 60870-5-104

از منظر امنیت سایبری

تالیف و گردآوری :

محمد مهدی احمدیان

بابک رضا زاده

- معرفی استاندارد IEC 60870-5-104
- بررسی تهدیدات، مخاطرات و آسیب پذیری های مرتبط با پروتکل IEC 60870-5-104
- راهکارهای امن سازی در مرحله طراحی پروتکل IEC 60870-5-104
- چک لیست ارزیابی امنیتی حوزه پروتکل IEC 60870-5-104

پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری

پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری

تالیف و گردآوری:

محمد مهدی احمدیان مرج، بابک رضازاده ابرندآبادی

انتشارات انستیتوایزایران

نام کتاب: پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری

مؤلف: محمدمهدی احمدیان مرج، بابک رضازاده ابرندآبادی

نوبت چاپ: اول – پاییز ۹۶

شمارگان: ۱۰۰۰ جلد

قیمت: ۲۲۰۰۰۰ ریال

شابک: ۹۷۸-۹۶۴-۲۰۱-۰۹۵-۰

طراح جلد: سعید بوذری

خیابان میرداماد – خیابان شهید حصاری (رازان جنوبی) پ ۳۶
تلفن: ۲۲۲۵٤۰۷۸ نمابر : ۲۲۲۲۵۲۶۵
www.isibook.ir

پیشگفتار

کتاب پیش رو با عنوان «پروتکل کنترل صنعتی IEC 60870-5-104 از منظر امنیت سایبری» حاصل مطالعه و پژوهش در حوزه پروتکل کنترل صنعتی IEC 60870-5-104 است. این کتاب با هدف تسهیل فرآیند شناخت جوانب امنیتی مختلف در رابطه با این پروتکل گردآوری و تألیف شده است؛ از این رو در این کتاب تلاش شده است تا ضمن بررسی عملیاتی پروتکل هدف، غالب اسناد، تحقیقات و پروژه‌های انتشار یافته عمومی مرتبط با موضوع این کتاب (تا تاریخ انتشار کتاب) گردآوری و مورد بررسی قرار گیرد. این کتاب در قالب چهار فصل به رشته تحریر در آمده است؛ در هر فصل ابتدا هدف فصل و مقدمه آن بیان می‌شود سپس تعاریف اولیه مرتبط با فصل ارائه می‌شوند. در ادامه محتوای فصل بیان شده و در انتهای هر فصل منابع به کار رفته در آن فصل جهت مطالعه بیشتر درج شده‌اند.

مخاطب این کتاب استفاده کنندگان و توسعه دهندگان محصولاتی می‌باشند که از پروتکل نامبرده استفاده می‌کنند یا درگیر پیاده سازی آن هستند اما نیازمندی امنیتی را نیز در کنار عملکرد اصلی این پروتکل مد نظر دارند. این کتاب به گونه‌ای به رشته تحریر در آمده است که برای هر دو قشر فارغ التحصیل رشته‌ی برق و رشته‌ی کامپیوتر قابل استفاده باشد. بخشی از این کتاب می‌تواند برای مدیران و مجریان به منظور درک عمیق‌تر چالش‌های امنیتی پروتکل نامبرده و تجهیزاتی که از آن بهره می‌برند یا با آن در ارتباط هستند به کار گرفته شود. باید به این احتمال نیز توجه کرد که برخی از محتویات این کتاب که برگرفته از برخی استانداردها می‌باشند ممکن است مشمول قوانین حق ثبت اختراع بین‌المللی باشند، در این سند حق اصالت این‌گونه موارد با ارجاع به منبع اصلی حفظ گردیده است. انتشار محتویات ارائه شده در این کتاب هیچ گونه مسئولیتی بابت صدمات فردی، خسارت دارایی یا دیگر خسارت‌ها به هر شکل ممکن، خواه مستقیم یا غیر مستقیم بر عهده شرکت [حذف در نسخه الکترونیکی] و نویسندگان این اثر نخواهد داشت؛ لذا توصیه می‌شود به مراجع اصلی ارجاع داده شده در کتاب و الزامات عملکردی و پایداری آن‌ها توجه شود.

محمد مهدی احمدیان[1] ، بابک رضا زاده[2]

[1]کاندیدای دکتری تخصصی IT(امنیت اطلاعات) دانشگاه صنعتی امیر کبیر
[2] دانشجوی دکتری تخصصی برق(کنترل) دانشگاه تربیت مدرس
مهرماه ۱۳۹۶

فهرست مطالب

مقدمه

در سال‌های اخیر با گسترش فناوری شاهد توسعه و به‌کارگیری فراگیر انواع سامانه‌های کنترل صنعتی در زیرساخت‌های حیاتی کشور بوده‌ایم. امروزه از جوانب مختلف، سامانه‌های کنترل صنعتی تأثیرات ویژه‌ای بر زندگی روزانه ما می‌گذارند و این روند به شکل روزافزون در حال گسترش است. انتظار می‌رود سامانه‌های کنترل صنعتی که در زیرساخت‌های حیاتی کشورها مورد استفاده قرار می‌گیرد، چالش‌ها و آسیب‌پذیری‌های امنیتی کمی داشته باشند، این در حالی است که واقعیت به گونه‌ی دیگری است. متخصصین امنیتی کشورهای مختلف دنیا نیز به شدت نگران تهدیدات و مخاطرات امنیتی این نوع سامانه‌ها هستند.

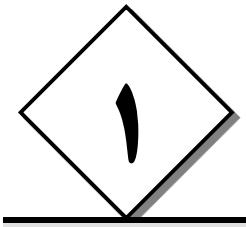
کتاب حاضر نمونه بارز بررسی موفق یکی از چالش‌های امنیتی سامانه‌های کنترل صنعتی است؛ این کتاب به شکل مفصل جزئیات پروتکل IEC 60870-5-104 از منظر امنیت سایبری را تشریح می‌نماید و از ابعاد مختلف، مسائل امنیتی آن را موشکافی می‌نماید. تألیف و گردآوری این کتاب گامی مهم در راستای معرفی تهدیدات، مخاطرات و آسیب‌پذیری‌های امنیتی مرتبط با پروتکل نامبرده به مسئولان سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی کشور، محققان، کارشناسان و دانشجویان فعال در این حوزه است، که می‌تواند الگویی برای بررسی و شناسایی مخاطرات امنیتی سایر پروتکل‌های ارتباطی این حوزه نیز باشد.

قاعدتاً شناخت مسائل موجود در این کتاب به مدیران، متولیان و مسئولان سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی کشور کمک می‌کند تا به چالش‌های مرتبط با پروتکل‌های شبکه‌های کنترل صنعتی به ویژه پروتکل نامبرده اشراف مناسبی پیدا کنند. از سویی دیگر این کتاب به کارشناسان فناوری اطلاعات، کارشناسان امنیت اطلاعات، کارشناسان و متخصصین شبکه‌های کنترل صنعتی و زیرساخت‌های حیاتی کشور کمک می‌کند تا برخی راه‌حل‌های امن سازی پروتکل هدف و پروتکل‌های مشابه را در مرحله طراحی بهتر بیاموزند و درزمینه امن سازی پروتکل‌های کنترل صنعتی، بومی سازی امن آن‌ها و ارائه پروتکل امن کنترل صنعتی دید مناسبی پیدا نمایند. در اینجا از [حذف در نسخه الکترونیکی] و نویسندگان محترم به خاطر اهتمام در این مهم قدردانی می‌نمایم و امید است بتوان به

حول قوه الهی با پشتکار و تلاش روزافزون، گامی مهم در راستای ارتقاء امنیت سامانه‌های کنترل صنعتی و زیرساخت‌های حیاتی کشور برداریم.

[حذف در نسخه الکترونیکی]

هاشم حبیبی



معرفی استاندارد IEC 60870-5-104

۱-۱- هدف فصل

در فصل نخست تلاش شده است تا بر اساس اسناد مرجع، معرفی مختصر و مطلوبی از استاندارد IEC 60870-5-104، ارائه گردد و زیر ساخت مناسبی برای درک بهتر چالش‌های امنیتی آن که در سایر فصول کتاب ارائه می‌شود فراهم شود. شایان ذکر است که این فصل صرفاً درآمدی بر پروتکل نامبرده خواهد بود و جایگزین اشراف به جزئیات این پروتکل که به واسطه اسناد مرجع این فصل قابل حصول است نخواهد بود.

۲-۱- مقدمه

سامانه‌های کنترل صنعتی که در صنعت و زیر ساخت‌های حیاتی کشورها مورد استفاده قرار دارند، اغلب توسط شرکت‌های محدود و انحصاری تولید می‌گردند. این سامانه‌ها در گذشته به صورت جدا از سایر سامانه‌های دیگر و از جمله شبکه‌های جهانی اینترنت به کار گرفته می‌شدند و این امر روشی در امن سازی این سامانه‌ها قلمداد می‌گردید. اتکا فراوان به این ممیزه، تولیدکنندگان و مصرف کنندگان این سامانه‌ها را از پرداختن به سایر لایه‌های امنیتی غافل کرده بود. استفاده از معماری و پروتکل‌های غیر امن و واسط‌های غیر استاندارد را می‌توان از نتایج این رویکرد دانست.

به دلیل نیازمندی‌های جدید و توسعه فناوری امروزه این قبیل سامانه‌های صنعتی، به تدریج با انواع جدیدتر جایگزین و یا به روز رسانی می‌گردند. در سامانه‌های جدید از پروتکل‌ها و نقاط دسترسی ارتباطی مشترک در شبکه‌ها استفاده می‌گردد که این امر موجب دسترسی مستقیم و غیر مستقیم به این سامانه‌ها از طریق شبکه‌های اختصاصی و یا اینترنت گردیده و آن‌ها را همانند سایر محصولات درگیر با فناوری‌های اطلاعات در مقابل تهدیدات سایبری آسیب پذیر نموده است. در مواجهه با این تهدیدات که روز به روز در حال افزایش هستند، اقدامات متعارفی نظیر اطلاع رسانی امنیتی، اتخاذ خط مشی‌های[۱] امنیتی موثر و سایر فعالیت‌های مقتضی با تأخیر به این حوزه ورود یافته و پرداختن به این قبیل موارد را اجتناب ناپذیر نموده است. گسترش روز افزون شبکه‌های ارتباطی، امنیت آن‌ها به چالش مهمی برای شرکت‌ها و سازمان‌های مختلف تبدیل شده است. نصب انواع تجهیزات امنیتی نظیر ضد بدافزارها[۲] دیواره‌های آتش، سامانه‌های تشخیص نفوذ و راه اندازی تونل‌های امن اختصاصی، جداسازی منطقی شبکه‌ها[۳] و راهکارهای دیگر به این منظور استفاده می‌شوند. یکی از بخش‌هایی که به دلیل درگیری اجزای مختلف سایبری و فیزیکی از شبکه به شکل وسیع برای ارتباط بین تجهیزات مختلف استفاده می‌کند، محیط‌های صنعتی[۴] می‌باشد. امروزه محیط‌های صنعتی به عنوان یکی از مهم‌ترین کاربردهای سامانه‌های سایبر–فیزیکی (CPS)[۵] مطرح است [1]. شبکه مورد استفاده در محیط‌های صنعتی را اصطلاحاً شبکه‌های صنعتی[۶] می‌گویند.

زمانی که سامانه‌های اسکادا[۷] (سامانه کنترل سرپرستی و گردآوری داده که در این کتاب از واژه اسکادا برای اطلاق به آن استفاده می‌کنیم) طراحی و پیاده سازی شد، میزان ارتباطات این نوع سامانه

---

۱ Policy

۲ Anti-Malwares

۳ Network Logical Isolation (Air Gaps)

۴ Industrial Enviroment

۵ Cyber Physical System

۶ Industrial Network

۷ SCADA: Supervisory Control and Data Acquisition

با سایر شبکه‌ها در کمترین میزان ممکن بود یا اصلاً هیچ ارتباطی با شبکه‌های دیگر نداشت. با توسعه سامانه‌های

[بقیه محتوا در نسخه تبلیغاتی کتاب حذف شده است]

حسن ختام

در این اثر در قالب چهار فصل تلاش شد تا ضمن معرفی مختصری از استاندارد T104 فرآیند شناخت جوانب امنیتی مختلف در رابطه با این پروتکل حاصل شود. در فصل نخست تلاش شد تا بر اساس اسناد مرجع، معرفی مختصر و مطلوبی از استاندارد T104 ارائه گردد و زیر ساخت مناسبی برای درک بهتر چالش‌های امنیتی آن که در سایر فصول کتاب گردید فراهم شود. در فصل دوم تلاش شد تا ضمن بیان تعاریف اولیه از مباحث امنیت سایبر–فیزیکی به کار رفته در مطالب کتاب، بر اساس ساختار استاندارد T104 مرجع و برخی محصولات پیاده سازی شده، آسیب‌پذیری‌ها و تهدیدات این پروتکل استخراج و معرفی گردند؛ در ادامه این فصل بر اساس اسناد فنی و راهنمای موجود آموختیم که چگونه آسیب‌پذیری‌های معرفی شده در مرحله پیاده سازی و پیکربندی را رفع نماییم.

در فصل سوم تلاش شد تا بر اساس اسناد مرجع که ملاحظات عملکردی و پایداری کنترلی را نیز در نظر می‌گیرند برخی راهکارهای امن سازی مرحله طراحی پروتکل T104 را بررسی کنیم؛ قاعدتاً شناخت مسائل درگیر در این فصل به ما کمک می‌کند تا برخی راه‌حل‌های امن سازی پروتکل T104 و پروتکل‌های مشابه را در مرحله طراحی بهتر بیاموزیم و چنانچه قصد داشته باشیم در آینده در زمینه امن سازی پروتکل‌های کنترل صنعتی، بومی سازی امن آن‌ها و ارائه پروتکل کنترل صنعتی جدید امن فعالیت کنیم بتوانیم الگوهای مناسبی برای این حوزه پژوهشی و صنعتی داشته باشیم. در فصل چهارم چک لیست ارزیابی تجهیزات مرتبط با پروتکل T104 به منظور ارزیابی امنیتی واحدهای کنترل صنعتی و فرآیندهای صنعتی که از این پروتکل استفاده می‌کنند طراحی شده است.

با استناد به محتوای کتاب و با مرجع قرار دادن استانداردهای مرجع [٤٤] و [٢٣] می‌توان در عمل پروتکل T104 را تا حد مطلوبی امن سازی کرد، اما این به معنای تضمین امنیت ١٠٠٪ در این پروتکل نیست چرا که هنوز این دو مرجع برخی ضعف‌های امنیتی مطرح شده را برطرف نکرده‌اند و از سوی دیگر چنانچه این ضعف‌های در سال‌های بعد برطرف شوند باز هم در عمل امنیت با تضمین ١٠٠٪ تحقق پیدا نخواهد کرد.

انتشار این اثر به معنی ادعای ارائه راه حل جامع امنیتی پروتکل T104 نیست بلکه تلاش شد تا بتوانیم در حد بضاعت خود چالش‌ها و مشکلات امنیتی این پروتکل را استخراج کنیم و تا حد ممکن راه‌حل‌هایی برای کاهش مخاطرات امنیتی این پروتکل ارائه کنیم. ادعایی نیست که این اثر، عاری از نقص باشد، پیشاپیش همه‌ی قصورات و کاستی‌های آن را می‌پذیریم و ضمن پوزش، انتقادات و پیشنهادات شما را با آغوشی باز و با افتخار پذیرا هستیم.

جهت ارتباط با نویسندگان کتاب می‌توانید از آدرس ذیل استفاده کنید:

MM.Ahmadian@aut.ac.ir
http://www.MMAhmadian.ir/

From Cyber Security Perspective, IEC 60870-5-104 Industrial Control System Protocol

این کتاب با هدف تسهیل فرآیند شناخت جوانب امنیتی مختلف در رابطه با پروتکل IEC60870-5-104 گردآوری و تالیف شده است؛ در این کتاب تلاش شده است تا ضمن بررسی عملیاتی پروتکل هدف، غالب اسناد، تحقیقات و پروژه‌های انتشار یافته عمومی مرتبط با موضوع این کتاب گردآوری و مورد بررسی قرار گیرد. مخاطب این کتاب استفاده کنندگان و توسعه دهندگان محصولاتی می‌باشند که از پروتکل نامبرده استفاده می‌کنند یا درگیر پیاده سازی آن هستند اما نیازمندی امنیتی را نیز در کنار عملکرد اصلی این پروتکل مد نظر دارند. این کتاب به گونه‌ای به رشته تحریر در آمده است که برای هر دو قشر فارغ التحصیل رشته‌ی برق و رشته‌ی کامپیوتر قابل استفاده باشد. بخشی از این کتاب می‌تواند برای مدیران و مجریان به منظور درک عمیق تر چالش‌های امنیتی پروتکل نامبرده و تجهیزاتی که از آن بهره می‌برند یا با آن در ارتباط هستند به کار گرفته شود.