فصلنامه علمی-ترویجی پدافند غیرعامل
سال ششم، شماره ۴، زمستان ۱۳۹۴، (پیاپی ۲۴): صص ۳۱-۲۳

ارائه یک مدل مفهومی جامع برای آسیب‌پذیری‌های سیستم کنترل واحدهای صنعتی و زیرساخت‌های حیاتی

احمد افشار[۱]، عاطفه ترمه‌چی[۲]، عارفه گلشن[۳]، آزاده آقائیان[۴]، حمیدرضا شهریاری[۵]، ساجده سلیمانی[۶]

تاریخ دریافت: ۹۳/۰۵/۱۱
تاریخ پذیرش: ۹۴/۰۳/۲۰

چکیده

استفاده از فناوری اطلاعات و رایانه که به‌منظور افزایش کیفیت، کارایی و ضریب اطمینان در سیستم‌های کنترل صنعتی و اتوماسیون به‌کار می‌رود، تهدیدات ناخواسته‌ای نظیر حمله‌های سایبری را متوجه این سیستم‌ها کرده است. یکی از مهم‌ترین قدم‌ها در امن کردن سیستم‌های کنترل صنعتی، شناسایی آسیب‌پذیری‌های آن‌ها می‌باشد. سیستم‌های کنترلی با توجه به عملکرد متفاوت قسمت‌های مختلف آن، به‌صورت لایه‌ای توصیف می‌شوند و با توجه به عملکرد و نحوه ارتباط لایه‌های مختلف، آسیب‌پذیری‌های آن‌ها نسبت به حملات سایبری گسترده و متفاوت می‌باشند. همچنین به‌منظور رفع این آسیب‌پذیری‌ها اقدامات امنیتی متفاوتی نیز باید اعمال گردد. با توجه به گستردگی آسیب‌پذیری‌های سیستم کنترل و همچنین نبود یک مدل مفهومی جامع آسیب‌پذیری مبتنی بر ساختار سیستم کنترل، هدف این مقاله دسته‌بندی و ارائه یک مدل مفهومی جامع برای آسیب‌پذیری‌های سیستم کنترل می‌باشد؛ که با استفاده از دسته‌بندی‌های ارائه‌شده برای آسیب‌پذیری‌ها در استانداردها و توصیه‌نامه‌های رایج امنیتی و همچنین با توجه به ساختار لایه‌ای این سیستم‌ها تهیه شده است تا با کمک آن بتوان اقدامات امنیتی بهینه‌ای را به‌منظور کاهش و یا از بین بردن آسیب‌پذیری‌ها تدوین کرد. در نهایت، مدل مفهومی ارائه‌شده می‌تواند به شناسایی آسیب‌پذیری‌ها و دریچه‌های نفوذ در سیستم‌های کنترل صنعتی کمک کرده و تا حد امکان از بروز حملات سایبری جلوگیری نماید.

کلیدواژه‌ها: سیستم کنترل، حمله سایبری، آسیب‌پذیری، مدل مفهومی

۱- دانشیار دانشگاه صنعتی امیرکبیر، پژوهشکده پدافند غیرعامل-aafshar@aut.ac.ir- نویسنده مسئول
۲- کارشناس ارشد دانشگاه صنعتی امیرکبیر، پژوهشکده پدافند غیرعامل
۳- کارشناس ارشد دانشگاه صنعتی امیرکبیر، پژوهشکده پدافند غیرعامل
۴- کارشناس ارشد دانشگاه صنعتی امیرکبیر، پژوهشکده پدافند غیرعامل
۵- استادیار دانشگاه صنعتی امیرکبیر، پژوهشکده پدافند غیرعامل
۶- کارشناس دانشگاه صنعتی امیرکبیر، پژوهشکده پدافند غیرعامل

۱- مقدمه

امروزه کلیه زیرساخت‌های حیاتی، واحدهای صنعتی و تجهیزات مدرن شهری و کشوری از سیستم‌های کنترل و اتوماسیون مبتنی بر شبکه، برای پایش و کنترل فرآیندهای خود استفاده می‌نمایند. به بیان دیگر، سیستم‌های کنترل و اتوماسیون، نقش مغز و سیستم عصبی پیکره زیرساخت‌های حیاتی و سیستم‌های صنعتی را ایفا می‌کنند. با پیشرفت سیستم‌های کنترل و استفاده آن‌ها از سکوهای نرم‌افزاری، سخت‌افزاری و شبکه‌ای یکسان و دارای استانداردهای واحد، امکان دسترسی افراد غیرمجاز به لایه‌های درونی این سیستم‌ها بسیار آسان شده و آن‌ها را از جانب تهدیدهای سایبری آسیب‌پذیر نموده است.

به‌طور کلی مهاجمی که قصد آسیب به یک سیستم کنترل را دارد، با سه چالش عمده مواجه است:

۱) نفوذ و دسترسی به سیستم کنترل

۲) بررسی کلی و شناسایی سیستم

۳) در دست گرفتن کنترل کل یا قسمتی از فرآیند

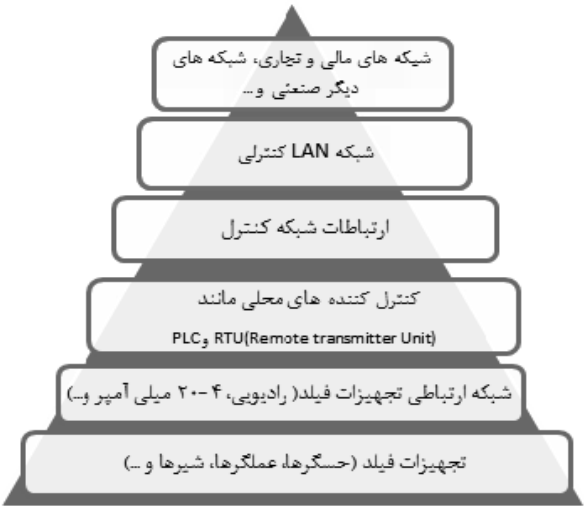
به‌منظور امن کردن یک سیستم کنترل صنعتی، یکی از مهمترین قدم‌ها، شناسایی آسیب‌پذیری‌ها و نقاط نفوذ به آن می‌باشد. آسیب‌پذیری‌های یک سیستم، ضعف‌ها یا نقص‌های موجود در طراحی، پیاده‌سازی، به‌کارگیری یا مدیریت یک سیستم می‌باشد که می‌تواند به منظور اختلال در تمامیت یک سیستم یا سیاست امنیتی آن مورد سوءاستفاده قرار بگیرد [۱]. لازمه شناسایی آسیب‌پذیری‌های یک سیستم کنترل، اطلاع از انواع فرآیندها و ارتباطات آن می‌باشد؛ به علاوه، آگاهی از این که مهاجمان چگونه می‌توانند از نقاط ضعف سیستم برای پیشبرد اهداف خود استفاده نمایند [۲]. با توجه به تنوع تجهیزات نرم‌افزاری، سخت‌افزاری و ساختاری سیستم‌های کنترل، آسیب‌پذیری‌های موجود در این سیستم‌ها نیز بسیار گسترده و متنوع می‌باشند. بنابراین، داشتن ساختاری جامع به‌منظور دسته‌بندی این آسیب‌پذیری‌ها بسیار ضروری می‌باشد. در دسته‌بندی ارائه‌شده در مرجع [۳]، این آسیب‌پذیری‌ها به سه دسته آسیب‌پذیری‌های مدیریت و استراتژی، آسیب‌پذیری‌های سکوها و آسیب‌پذیری‌های شبکه‌ای تقسیم‌بندی شده‌اند. با توجه به تعریف و شرح ارائه‌شده برای هر کدام از این سه دسته، یکی از ضعف‌های این دسته‌بندی، وجود اشتراکات و همپوشانی بین زیردسته‌ها می‌باشد. از سوی دیگر، در شرح و تعریف هیچ‌یک از دسته‌ها و زیردسته‌های آن‌ها، ساختار و آسیب‌پذیری‌های خاص سیستم کنترل مانند آسیب‌پذیری‌های موجود در ساختار و الگوریتم‌های ناامن کنترلی مورد توجه قرار نگرفته است. همچنین با توجه به گستردگی و تنوع دارایی های موجود در دسته آسیب‌پذیری‌های سکوها، توجه به این نکته ضروری است که این دسته خود نیازمند یک دسته‌بندی مجدد با توجه به ساختار سیستم کنترل و مدل دارایی‌های آن می‌باشد. در مراجع [۶-۴] مدل‌هایی از دارایی‌ها و ساختار ارتباطی سیستم‌های کنترل صنعتی عمومی و خاص، بر اساس ساختار لایه‌ای آن‌ها، پیشنهاد شده است. در این مقاله سعی شده است یک مدل مفهومی جامع برای آسیب‌پذیری‌های سیستم کنترل واحدهای صنعتی و زیرساخت‌های حیاتی ارائه شود. این مدل مفهومی بر اساس مفاهیم و دسته‌بندی‌های ارائه‌شده برای آسیب‌پذیری‌ها در استانداردها و توصیه‌نامه‌های رایج در زمینه امنیت سایبری سیستم‌های صنعتی [۱، ۳ و ۱۲-۵] و همچنین با توجه به ساختار عملکردی و لایه‌ای سیستم‌های کنترل پیشنهاد شده است. در این مقاله آسیب‌پذیری‌های این سیستم‌ها به سه دسته کلی آسیب‌پذیری‌های سیاست‌ها و رویه‌های امنیتی، آسیب‌پذیری‌های ساختاری شبکه کنترل و آسیب‌پذیری‌های تجهیزات و پروتکل‌های ارتباطی شبکه کنترل تقسیم‌بندی می‌شوند. هر دسته از این مدل مفهومی، خود شامل طیف گسترده‌ای از آسیب‌پذیری‌ها می‌باشد که به پاره‌ای از آن‌ها اشاره می‌شود.

۲- سیستم‌های کنترل و اتوماسیون صنعتی

سیستم‌های کنترل صنعتی، سیستم‌هایی هستند که وظیفه هدایت و کنترل فرآیندهای فیزیکی را بر عهده دارند. این سیستم‌ها معمولاً متشکل از مجموعه‌ای از اجزای متعدد شامل حسگرها، عملگرها، واحدهای پردازش داده مانند کنترل‌کننده‌های منطقی قابل برنامه‌ریزی (PLCs)، شبکه‌های ارتباطی و رایانه‌های مرکزی می‌باشند [۱۴-۱۳].

چندین روش استاندارد برای تبیین ساختار سیستم کنترل صنعتی وجود دارد. این مقاله یک ساختار لایه‌ای با الهام از

استاندارد [۷ و ۱۳] ISA[1] مطابق شکل (۱) پیشنهاد می‌دهد:



شکل ۱- لایه‌های یک شبکه کنترل صنعتی

لایه اول، لایه تجهیزات فیلد[2]: تجهیزات فیلد که با سیستم فیزیکی تحت کنترل در ارتباط هستند مانند حسگرها و عملگرها.

حسگرها: وظیفه دریافت شرایط سیستم فیزیکی تحت کنترل مانند دما، فشار، سرعت، توان و ... را به عهده دارند.

عملگرها: این اجزاء مانند پمپ‌ها، شیرهای کنترل و نقاله‌ها به‌وسیله سیستم کنترل و رله‌ها فعال می‌شوند.

لایه دوم، شبکه ارتباطی فیلد: وظیفه ارتباط میان پردازشگر محلی و حسگرها یا عملگرها و یا ارتباط میان خود حسگرها و عملگرهای واقع در فیلد را به عهده دارد، این ارتباطات از طریق کابل‌ها یا اتصالات بی‌سیم برقرار می‌شود. این داده‌های ارتباطی به شکل سیگنال‌های آنالوگ به صورت ولتاژ یا جریان و یا به شکل سیگنال‌های دیجیتال به‌صورت بیت‌های دیجیتال در قالب پروتکل‌های صنعتی می‌باشند. این ارتباطات معمولاً برد کوتاه هستند.

لایه سوم، کنترل‌کننده‌های محلی: پردازشگر رابط بین حسگرها و عملگرها در فیلد می‌باشد که پایش، پردازش و کنترل محلی را امکان‌پذیر می‌سازد. این پردازشگرها می‌توانند همه یا بخشی از وظایف زیر را برعهده داشته باشند:

- جمع‌آوری داده‌های اندازه‌گیری و تجهیزات فیلد
- خاموش یا روشن کردن عملگرها با توجه به برنامه منطقی[3] خود این پردازشگرها یا دستوراتی که از راه دور از طرف اپراتور یا رایانه اتاق کنترل مرکزی دریافت می‌کند.
- ترجمه پروتکل‌ها و زبان‌های متفاوت کنترل‌کننده، تجهیزات و ابزارهایی که با هم در ارتباط هستند.
- تشخیص شرایط هشدار و بحرانی

PLC[4]، RTU[5]، IED[6] و PAC[7] را می‌توان به عنوان پردازشگرهای محلی معرفی کرد. همچنین، یک پردازشگر محلی گاهی طوری طراحی می‌گردد که در مواقع اضطراری بتواند به تنهایی وظیفه هدایت و هماهنگی بین حسگرها و عملگرها را به عهده داشته باشد.

لایه چهارم، ارتباطات شبکه کنترل: که وظیفه برقراری ارتباط بین پردازشگرهای محلی و یا بین کنترل‌کننده محلی و مرکز کنترل را به عهده دارد. این ارتباطات ممکن است طی چندین کیلومتر و از طریق خطوط تلفن، ارتباطات رادیویی، ماکروویو، شبکه‌های سلولی، ماهواره و ... برقرار گردند.

لایه پنجم، شبکه LAN کنترلی: هسته اصلی هر سیستم کنترل صنعتی، مرکز کنترل آن می‌باشد که در واقع نقطه ثقل و مرکزی کنترل و پایش سیستم است و از یک یا تعداد بیشتری رایانه میزبان برای ارائه نمایش‌های گرافیکی و امکانات محاسباتی و شبکه‌ای بهره می‌برد. رایانه‌های میزبان در محلی واقع هستند که اپراتور انسانی را قادر به نظارت فرآیند و دریافت هشدارها و بررسی داده‌ها و عملیات کنترل می‌سازد. در حالی که این رایانه‌ها می‌توانند دارای برنامه منطقی خاص خود به منظور کنترل پردازشگرهای منطقی محلی باشند، در برخی موارد ممکن است تنها به عنوان رابط بین پردازشگرهای محلی و اپراتور به کار روند. وظیفه دیگر رایانه‌های میزبان، ذخیره اطلاعات در پایگاه داده[8] و ثبت تاریخچه عملکرد سیستم می‌باشد. سخت‌افزار رایانه میزبان، اغلب یک PC صنعتی استاندارد است.

لایه ششم، شبکه مالی تجاری: مجموعه‌ای از اجزای فناوری اطلاعات (سخت‌افزار، نرم‌افزار و سرویس‌ها) که با هدف انجام فرآیندهای مالی تجاری و یا ارتباط با شبکه‌های کنترلی دیگر به‌کار گرفته می‌شوند.

1- International Society of Automation
2- Field

3- Logic Program
4- Programmable Logic Controller
5- Intelligent Electronic Device
6- Artificial Bee Colony
7- Process Automation Controller
8- Database

۳- مدل مفهومی آسیب‌پذیری‌های یک سیستم کنترل صنعتی

آسیب‌پذیری‌های یک سیستم کنترل صنعتی را می‌توان به سه دسته کلی زیر تقسیم‌بندی کرد:

- آسیب‌پذیری‌های سیاست‌ها و رویه‌های امنیتی
- آسیب‌پذیری‌های ساختاری شبکه کنترل صنعتی
- آسیب‌پذیری‌های تجهیزات و پروتکل‌های ارتباطی سیستم کنترل

۳-۱- آسیب‌پذیری‌های سیاست‌ها و رویه‌های امنیتی

بنیان هر برنامه امنیتی، سیاست‌ها و رویه‌های امنیتی آن برنامه می‌باشد. علت اصلی اغلب آسیب‌هایی که متوجه یک سیستم کنترل صنعتی می‌شود، عدم وجود سیاست‌ها و رویه‌های امنیتی کامل و مناسب در این سیستم‌ها می‌باشد [۳]. از جمله این آسیب‌پذیری‌ها می‌توان به موارد زیر اشاره کرد:

- نبود برنامه مناسب جهت مدیریت تغییرات در این سیستم‌ها
- نبود برنامه‌های آموزشی مناسب
- عدم تعریف دقیق فعالیت‌ها و فرآیندهای مجاز
- عدم برنامه‌ریزی به‌منظور ارزیابی امنیتی منظم اشاره کرد.

۳-۲- آسیب‌پذیری‌های ساختاری شبکه کنترل صنعتی

یک مهاجم می‌تواند نفوذ خود را از طریق آسیب پذیری‌های موجود در ساختار شبکه کنترل، تحقق و گسترش بخشد. دسته آسیب پذیری های ساختاری شبکه کنترل، به آسیب پذیری هایی اشاره دارد که ناشی از ضعف ساختاری شبکه کنترل شامل ساختار اتصالی ناامن و یا ضعف ساختار منطق کنترلی شبکه می‌باشد. از جمله آسیب‌پذیری‌های موجود در این دسته می‌توان به موارد زیر اشاره کرد:

- ضعف امنیتی در ساختار اتصالی بین تجهیزات یک شبکه کنترل و یا بین یک شبکه با شبکه‌های دیگر
- اتصال غیرضروری شبکه به شبکه‌های نا امن
- الگوریتم‌های نا امن کنترلی

پژوهش‌ها و مقالات زیادی در راستای شناسایی و رفع آسیب‌پذیری‌های موجود در الگوریتم‌های کنترلی انجام شده است. نویسندگان در مرجع [۱۵] مروری بر این پژوهش‌ها و مقالات ارائه کرده‌اند.

۳-۳- آسیب‌پذیری‌های تجهیزات و پروتکل‌های ارتباطی سیستم کنترل

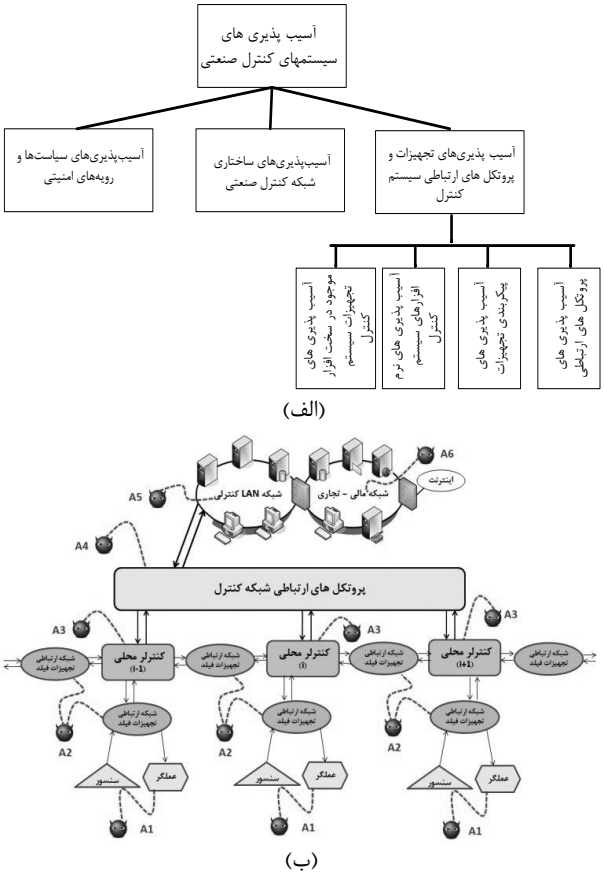
این دسته از آسیب‌پذیری‌ها شامل:

- آسیب‌پذیری‌های موجود در سخت‌افزار تجهیزات سیستم کنترل
- آسیب‌پذیری‌های نرم‌افزارهای سیستم کنترل
- آسیب‌پذیری‌های پیکربندی تجهیزات
- آسیب‌پذیری‌های پروتکل‌های ارتباطی

با توجه به گستردگی و تنوع دارایی‌های موجود در این دسته، همچنین با عنایت به ساختار عملکردی و لایه‌ای سیستم‌های کنترل و مدل ساختاری بیان‌شده در قسمت قبل، این دسته از آسیب‌پذیری‌ها به شش زیردسته تقسیم‌بندی می‌شود:

۱. آسیب‌پذیری‌های سخت‌افزاری، نرم‌افزاری و پیکربندی تجهیزات فیلد
۲. آسیب‌پذیری‌های پروتکل‌های ارتباطی تجهیزات فیلد
۳. آسیب‌پذیری‌های سخت‌افزاری، نرم‌افزاری و پیکربندی کنترل‌کننده‌های محلی مانند RTU، PLC
۴. آسیب‌پذیری‌های پروتکل‌های ارتباطی شبکه کنترل
۵. آسیب‌پذیری‌های سخت‌افزاری، نرم‌افزاری و پیکربندی تجهیزات شبکه LAN کنترلی
۶. آسیب‌پذیری‌های سخت‌افزاری، نرم‌افزاری و پیکربندی تجهیزات و پروتکل‌های ارتباطی موجود در لایه اتصال به شبکه‌های همکار و مالی– تجاری

هدف نهایی، حمله به سیستم‌های کنترل، جاسوسی و یا صدمه به لایه فیزیکی می‌باشد و مهاجم ممکن است از طریق آسیب‌پذیری‌های لایه‌های مختلف، هدف خود را تحقق بخشد.



شکل ۲-مدل مفهومی آسیب‌پذیری‌های سیستم‌های کنترل صنعتی الف) آسیب‌پذیری‌های سیستم‌های کنترل صنعتی ب) دسته‌بندی آسیب‌پذیری‌های تجهیزات و پروتکل‌های ارتباطی سیستم کنترل با توجه به لایه‌ها و ساختار سیستم کنترل

۴- نمونه‌هایی از آسیب‌پذیری‌های هر دسته از مدل مفهومی

۴-۱- آسیب‌پذیری‌های سیاست‌ها و رویه‌های امنیتی

همانطور که بیان شد، علت اصلی اغلب آسیب‌هایی که متوجه یک سیستم کنترل صنعتی می‌شود، عدم وجود سیاست‌ها و رویه‌های امنیتی کامل و مناسب در این سیستم‌ها می‌باشد.

۴-۱-۱- عدم تعریف دقیق دسترسی‌ها و فرآیندهای مجاز

در بیشتر سیستم‌های کنترلی، مهندسان دسترسی کاملی به شبکه LAN کنترلی دارند. تزریق بدافزارها به سیستم به‌واسطه مهندسان و کارمندان، یکی از معمول‌ترین مکانیزم‌های حمله است.

۴-۲-آسیب‌پذیری‌های ساختاری شبکه کنترل صنعتی

- **اتصال به شبکه پشتیبانی فروشنده**

یکی از راه‌های نفوذ، از طریق پشتیبانی فروشنده امکان‌پذیر می‌شود. خریدار در هنگام ارتقاء یا به‌روزرسانی سیستم، از خدمات پس از فروش بهره‌مند می‌شود. متداول‌ترین نحوه پشتیبانی، از طریق مودم‌های ارتباطی است که در سال‌های اخیر، این ارتباط به VPN ارتقاء یافته است. مهاجم تلاش می‌کند تا به منابع داخلی فروشنده دسترسی پیدا کند و از آن برای ارتباط با LAN سیستم کنترلی استفاده نماید و یا مهاجم منتظر می‌ماند تا کاربری مورد اطمینان از طریق VPN به LAN سیستم کنترلی دسترسی یابد؛ سپس خود را سوار بر این ارتباط کرده و به این ترتیب به شبکه سیستم کنترلی نفوذ می‌کند.

۴-۲-۱- اتصال به زیرسیستم‌های مجاور

یک شبکه LAN کنترلی ممکن است تأسیسات و شبکه‌های کنترلی مجاور خود را نیز تحت کنترل داشته باشد یا به آن‌ها متصل باشد. در این صورت امنیت سیستم بسیار کاهش یافته و امکان نفوذ به این شبکه افزایش می‌یابد.

۴-۲-۲- اتصال به کنترل‌کننده محلی از طریق ارتباط تلفنی

یکی از رایج‌ترین مسیرهای انتقال اطلاعات به کنترل‌کننده‌ها، استفاده از مودم‌های ارتباط تلفنی است که نقش پشتیبان مسیرهای ارتباطی را دارند. مهاجم هر زیرخطی از کارخانه را می‌گیرد تا مودم‌های متصل به سیستم تلفن شرکت را بیابد. بیشتر کنترل‌کننده‌های محلی هیچ رمز عبوری برای تأیید لازم ندارند و بسیاری از آن‌ها همچنان با رمز عبور پیش‌فرض خود کار می‌کنند.

۴-۳- آسیب‌پذیری‌های تجهیزات و پروتکل‌های ارتباطی سیستم کنترل

۴-۳-۱- آسیب‌پذیری‌های سخت‌افزاری، نرم‌افزاری و پیکربندی تجهیزات فیلد

هدف نهایی بسیاری از حملات به سیستم کنترل، صدمه و ایجاد اختلال در عملکرد تجهیزات لایه فیلد می‌باشد. با توجه به روند رو به گسترش هوشمندی کامل تجهیزات لایه فیلد، از جمله سنسورها و عملگرها، نفوذ مستقیم بدافزارها به این لایه و استفاده از آسیب‌پذیری‌های سخت‌افزاری آن‌ها امکان‌پذیر شده است. به این

ترتیب مهاجمان با دسترسی به کدهای نرم‌افزاری و یا سفت‌افزاری[1] این تجهیزات، و استفاده از آسیب‌پذیری‌های آن‌ها، می‌توانند مستقیماً به هدف نهایی خود دست یابند.

در سال‌های اخیر، علاوه‌بر آسیب‌پذیری‌های نرم‌افزاری، آسیب‌پذیری‌های سخت‌افزاری و سفت‌افزاری نیز به شدت مورد توجه کارشناسان امنیت قرار گرفته است [۱۶-۲۲]. این نوع آسیب‌پذیری‌ها در پردازنده‌ها و قطعات الکترونیکی به‌طور گسترده وجود دارند و حتی در سطوح مخابراتی و یا نظامی نیز یافت می‌شوند. مانند وجود یک نقطه دسترسی مخفی در تراشه‌های ساخت یک شرکت چینی که در تجهیزات نیروی هوایی آمریکا به‌کار می‌روند [۲۳] و توسط تیم تحقیقاتی دانشگاه کمبریج شناسایی شده است [۱۴ و ۲۴]. عموماً این نوع تهدیدات به عنوان آسیب پذیری های درپشتی[2] در تجهیزات در نظر گرفته می‌شوند.

۴-۳-۲- آسیب پذیری های سخت افزاری، نرم افزاری و پیکربندی کنترل‌کننده‌های محلی مانند RTU، PLC

مهاجم ممکن است هدف خود را از طریق تحت کنترل درآوردن لایه کنترل‌کننده‌های محلی تحقق بخشد. یکی از مشهورترین حملاتی که از آسیب‌پذیری‌های سخت‌افزاری موجود در تجهیزات لایه کنترل محلی استفاده کرده است، حمله استاکس‌نت می‌باشد. مهاجمان با دسترسی به کد نرم‌افزاری و سخت‌افزاری این تجهیزات، می‌توانند به راحتی کنترل فرآیند سامانه را در دست گیرند[3]. منابع بسیاری [۱۷, ۲۵, ۲۶] آسیب‌پذیری‌های PLCها را مورد بررسی قرار داده‌اند که حاکی از شدت ضعف این ابزارها در حوزه امنیت سایبری می‌باشد. نمونه‌هایی از اشکالات امنیتی که برای همه اجزای کنترل به تازگی شناخته شده‌اند در [۲۷] موجود است. به عنوان مثال، می‌توان به آسیب‌پذیری PLCهای مدل Micrologix 1100 و MicroLogix 1400 اشاره کرد که توسط شرکت Allen Bradley تولید شده‌اند. این دو کنترل‌کننده، رمز مدیریتی خود را از طریق متن به هر کاربری که قصد اتصال به آن‌ها را دارد، ارسال می‌کنند. به این ترتیب مهاجم به راحتی می‌تواند به این کنترل‌کننده‌ها دسترسی یابد. همچنین این کنترل‌کننده‌ها تنها با دریافت IDکاربر ، بدون بررسی رمز عبور و احراز هویت آن، هر دستور کاربر را از راه دور دریافت و اجرا می‌کنند [۲۹- ۲۸].

کشور ما به طور گسترده اکثر تجهیزات کنترلی مانند انواع RTU، PLC و ...را از دیگر کشورها خریداری کرده و در سیستم‌های حیاتی، حساس و مهم به کار می‌بندد. بنابراین می‌توان گفت که به‌طور جدی از این نظر در خطر است.

۴-۳-۳- آسیب‌پذیری‌های پروتکل‌های لایه ارتباطی شبکه کنترل و لایه شبکه ارتباطی تجهیزات فیلد

با توجه به این که پروتکل‌های استفاده‌شده در لایه‌های ارتباطی شبکه کنترل و شبکه ارتباطی تجهیزات فیلد، مشترکات زیادی دارند و حتی گاهی کاملاً مشابه می‌باشند، در این بخش به بیان تعدادی از آسیب‌پذیری‌های مشترک این دو لایه پرداخته می‌شود. لازم به ذکر است که ملزومات امنیتی این دولایه کاملاً مشابه نبوده و این خود می‌تواند ناشی از تفاوت در نیازهای امنیتی تجهیزاتی باشد که از این دو لایه برای ارسال داده استفاده می‌کنند.

امروزه پروتکل‌های ارتباطی بسیار زیادی در سیستم‌های اتوماسیون و کنترل صنعتی استفاده می‌شوند (طبق گزارش انجمن گاز آمریکا[4] [۳۰] در حدود ۱۵۰ تا ۲۰۰ پروتکل اسکادا وجود دارد). بیشتر این پروتکل‌ها با هدف بالا بردن کارایی، قابلیت اطمینان در عملیات بلادرنگ و پشتیبانی از الزامات اقتصادی و عملکردی در سیستم‌های کنترل بزرگ طراحی شده‌اند. متأسفانه اکثر این پروتکل‌ها به جهت بالا بردن کارایی، از هر ویژگی غیرضروری از جمله ویژگی‌های امنیتی نظیر احراز اصالت و رمزنگاری صرف‌نظر کرده‌اند. از سوی دیگر، بسیاری از آن‌ها برای استفاده روی اترنت و اتصال به شبکه اینترنت توسعه داده شده‌اند و این موضوع، آن‌ها را در معرض حملات بیشتری قرار داده است [۳۱]. علاوه بر موارد ذکرشده، یکسان‌سازی این پروتکل‌ها در سال‌های اخیر، منجر به کسب اطلاعات بسیار دقیق مهاجمان از کارکرد و جزییات آن‌ها شده است. به این ترتیب مهاجمان با شناسایی آسیب‌پذیری‌های این پروتکل‌ها می‌توانند به بسته‌های داده دسترسی پیدا کرده و به دلخواه در آن‌ها تغییراتی ایجاد کنند. مانند حمله به سیستم کنترل آب و فاضلاب شهر کوئیزلند استرالیا در سال ۲۰۰۱ که با آشنایی مهاجم از پروتکل و با دخالت مستقیم انسان صورت پذیرفت [۳۲].

آسیب‌پذیری‌های پروتکل‌های ارتباطی شبکه کنترل، در منابع علمی متعددی [۳۹-۳۲] مورد بررسی قرار گرفته است. در منبع [۳۱] انواع پروتکل‌های صنعتی، آسیب‌پذیری‌ها و راه‌کارهای امنیتی

1– Firmware
2– Backdoor
۳- حمله به خطوط انتقال گاز سیبری (۱۹۸۲)، حمله استاکس نت (۲۰۱۰) و ...
4– Number of Tie Lines

آن‌ها بررسی می‌شود. یکی از پروتکل‌های بررسی‌شده در این منبع، پروتکل مودباس است. این پروتکل فاقد احراز اصالت، رمزگذاری و مجموع مقابله‌ای پیام‌ها[1] می‌باشد. خطرناک‌ترین ویژگی مودباس، قابلیت برنامه‌ریزی آن است که بسیاری از پروتکل‌های صنعتی، در این ویژگی با مودباس اشتراک دارند؛ چرا که این پروتکل‌ها برای برنامه‌ریزی کنترل‌کننده‌ها طراحی شده‌اند. بنابراین می‌توانند برای تزریق برنامه‌های مخرب در PLC ها و RTUها مورد استفاده قرار بگیرند. آسیب‌پذیری پروتکل مودباس به عنوان پرکاربردترین پروتکل صنعتی، در منابع دیگر [۳۱، ۳۶، ۳۸، ۴۰ و ۴۱] نیز تشریح شده است. منبع [۳۸] حمله منع خدمت به این پروتکل و نحوه عملکرد مهاجم را بررسی کرده است. در این منبع بیان می‌شود که با توجه به سریال بودن پروتکل Modbus و انتقال اطلاعات از فرمانده به فرمانبر از طریق TCP، این پروتکل در برابر حمله منع خدمت بسیار آسیب‌پذیر است. حمله منع خدمت تلاش می‌کند هم‌زمانی انتقال داده بین فرمانده و فرمانبر را از بین ببرد و با وارد کردن طوفانی از بسته‌های اطلاعاتی نامرتبط در سیستم انتقال داده، باعث ایجاد ترافیک داده شده و در نهایت، از بین رفتن هم‌زمانی شود. این بدافزار برای عملکرد مناسب باید دارای اجزای زیر باشد:

- سازنده بسته‌های داده[2]: که وظیفه ساختن بسته‌های داده‌ای Modbus TCP دارد.
- موتور شناسایی[3]: این عنصر وظیفه شناسایی آدرس IP فرمانبرها را در شبکه به عهده دارد.
- رساننده بسته اطلاعاتی[4] : این جزء وظیفه فرستادن پیام ساخته‌شده به فرمانبر خاصی است که بدافزار قصد حمله به آن را دارد.

بدافزار منع خدمت بدون داشتن راه‌انداز[5] مناسب قادر به ورود به سیستم نیست مگر آن که کدهای ویرانگر خود را روی رایانه‌ای نصب کند که با شبکه فیلد و به طور کلی سیستم SCADA به هر نحوی در ارتباط است.

۴-۳-۴- آسیب پذیری های سخت افزاری، نرم افزاری و پیکربندی تجهیزات شبکه LAN کنترلی

مهاجم می‌تواند حمله و نفوذ خود را با استفاده از آسیب‌پذیری‌های موجود در لایه شبکه LAN کنترلی، تحقق بخشد. در ادامه به بیان سه آسیب‌پذیری احتمالی در این لایه اشاره می‌شود:

۴-۳-۵- دیوارهای آتش با پیکربندی ضعیف

اولین قدمی که مهاجم باید برای دسترسی به شبکه LAN سیستم کنترلی بردارد، عبور از پدافندهای مرزی می‌باشد. در حال حاضر، سعی می‌شود شبکه‌های کنترل صنعتی به‌طور مستقیم از طریق اینترنت قابل دسترسی نباشند و از دیوار آتش برای جداسازی شبکه LAN مالی و تجاری از شبکه LAN سیستم کنترل صنعتی استفاده شود. به این ترتیب هکرها دور نگه داشته می‌شوند و شبکه سیستم کنترل صنعتی از کرم‌ها و سایر مشکلاتی که در LAN مالی و تجاری رخ می‌دهد، ایزوله می‌شود. ضعف موجود در پیکربندی دیوارهای آتش، ممکن است موجب برقراری ارتباط غیرمجاز تجهیزات سیستم کنترلی با شبکه LAN مالی و تجاری و یا اینترنت شود.

۴-۳-۶- آسیب‌پذیری در پایگاه داده

سیستم کنترل صنعتی به‌طور گسترده از دادگان به‌منظور انتقال، ذخیره داده‌ها و همچنین ارتباط با شبکه‌های دیگر و اینترنت استفاده می‌کند. اکثر دادگان‌ها از زبان SQL برای عملکردهای خود استفاده می‌کنند. بنابراین استفاده از فرمت‌های پنهانی و پروتکل‌های اختصاصی، کارایی مناسب و گسترده را برای حفاظت از سیستم‌های کنترل جدید ندارد. مهاجم ماهر می‌تواند به پایگاه داده شبکه LAN دسترسی یابد و با استفاده از دستورات SQL سرور پایگاه داده شبکه LAN، سیستم کنترلی را تحت کنترل خود دربیاورد. تمامی مودم‌های پایگاه داده در صورت عدم پیکربندی مناسب، در برابر این تهدید آسیب‌پذیر هستند.

۴-۳-۷- آسیب‌پذیری در واسط انسان و کاربر[6]

با توجه به این‌که اکثر واسط‌های انسان و کاربر مبتنی بر محیط‌های ویندوز و لینوکس می‌باشند، یکی دیگر از انواع آسیب‌پذیری‌های این لایه، دسترسی مهاجم به واسط انسان و کاربر از طریق نقاط نفوذ در محیط‌های ویندوز و لینوکس می‌باشد.

۴-۳-۸- شبکه‌های همکار و مالی- تجاری

با توجه به این‌که این لایه، یک شبکه معمول رایانه ای است، آسیب‌پذیری‌های آن نیز از همان دسته می‌باشد. این دسته آسیب‌پذیری‌ها به‌طور گسترده در منابع مختلفی بحث و بررسی

1– Message Checksum
2– Packet Builder
3– Discovery Engine
4– Packet Deliverer
5– Trigger
6– Human Monitoring Interface

شده است، از این‌رو در این مجال از پرداختن مجدد به آن‌ها اجتناب می‌شود.

۵- نتیجه‌گیری

امروزه شناخت مهاجمان از آسیب پذیری‌های سیستم‌های کنترل صنعتی باعث شده است این سیستم ها در معرض حملات بدافزاری بسیاری قرار گیرند. از این‌رو شناخت آسیب پذیری‌ها و دریچه‌های نفوذ به سیستم‌های کنترل صنعتی، امری ضروری است. هدف همه بدافزارهای صنعتی، جاسوسی و یا صدمه به لایه فیزیکی است ولی این هدف را ممکن است با استفاده از نفوذ و دسترسی به لایه‌های مختلف برآورده سازند. از این‌رو، این مقاله با توجه به ساختار لایه‌ای سیستم کنترل، آسیب‌پذیری‌ها و نقاط دسترسی به سیستم کنترل را به سه دسته تقسیم‌بندی کرده و به شرح و بیان نمونه‌هایی از هر دسته از جزئیات هر دسته پرداخته است.

تشکر و قدردانی

این مقاله در ضمن اجرای فاز مطالعاتی پروژه طراحی و پیاده‌سازی سامانه جامع مقابله با بدافزارها در سیستم‌های کنترل صنعتی و زیرساخت‌های حیاتی تهیه شده است. این پروژه در راستای طرح کلان ملی معماری و راه اندازی مرکز ملی دفاع سایبری و سامانه‌های زیرساختی فضای سایبری، در پژوهشکده پدافند غیرعامل دانشگاه صنعتی امیرکبیر در حال اجرا می‌باشد.

۶- مراجع

1. U.S. National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, Federal Information Processing Standards (FIPS) PUB 140-2, Section 2, Glossary of Terms and Acronyms, 2001.
2. Haimes, Y. Yacov, and C. G. Chittester, "A roadmap for quantifying the efficacy of risk management of information security and interdependent SCADA systems," Journal of Homeland Security and Emergency Management, vol. 2, no. 2, pp. 1-23, 2005.
3. Stouffer, Keith, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication, pp. 800-802, June 2011.
4. ISA, ANSI, ISA–99.00. 01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology Concepts and Models, International Society for Automation, 2007.
5. Wind Turbines, Part 25-1: Communications for monitoring and control of wind power plants Overall description of principles and models, IEC 61400–25-1, 2006.
6. American Petroleum Institute (API) energy, Pipeline SCADA Security, API standard 1164, American Petroleum Institute, 2009.
7. ISA99, ISA/IEC 62443 Series of Standards on Industrial Automation and Control Systems (IACS) Security, 2012.
8. International Organization for Standardization, ISO/IEC 27005: Information technology- Security techniques- Information security risk management, 2011.
9. ISO, Information technology- Security techniques- Information security management guidelines based on ISO/IEC 27002 for process control, systems specific to the energy utility industry, 2013.
10. Ross, Ron, and S. Katzke, "NIST Special Publication 800-53: Recommended Security Controls for Federal Information Systems," Gaithersburg, MD: National Institute of Standards and Technology (NIST), 2009.
11. American Petroleum Institute, "Security Guidelines for the Petroleum Industry," API, April 2005.
12. PA, CPNI Group, NISCC: Good Practice Guide Process Control And SCADA Security, 2005.
۱۳. افشار، احمد، ترمه‌چی، عاطفه، گلشن، عارفه ، آقائیان، آزاده، شهریاری، حمیدرضا، مروری بر امنیت سایبری سیستم‌های کنترل صنعتی، مجله کنترل، دوره ۸، شماره ۱، ۱۳۹۳.
14. A. Abbasi, "Critical Infrastructure Vulnerability Assessment and Protection from Protocol Layer to Hardware Layer," Master Thesis, Tsinghua University, Beijing, China, 2013.
15. S. E. Valentine, "PLC Code Vulnerabilities Through SCADA Systems," PhD. Thesis, University of South Carolina, 2013.
16. A. A. Cárdenas, S. Amin, Z. S. Lin, Y. L. Huang, C. Y. Huang, and S. Sastry, "Attacks against process control systems: risk assessment detection and response," roceedings of the 6th ACM symposium on information, computer and communications security, pp. 355-366, 2011.
17. K. Barnes, J. Briam, and N. Reva, "Introduction to SCADA protection and vulnerabilities," Idaho National Engineering and Environmental Laboratory, Tech. Rep. INEEL/EXT-04-01710, 2004.

18. J. Stidham, “Can hackers turn your lights off: The vulnerability of the US power grid to electronic attack,” SANS Institute, 2001.

19. R. Robles, C. Min-kyu, C. Eun-suk, K. Seok-soo, P. Gil-cheol, and S. Yeo, “Vulnerabilities in SCADA and critical infrastructure systems,” International Journal of Future Generation and Networking, vol. 1, no. 1, pp. 102-103, 2008.

20. R. Robles, J. Rosslin, and C. Min-kyu, “Assessment of the vulnerabilities of SCADA,” control systems and critical infrastructure systems, Assessment, vol. 2, no. 2, 2009.

21. S. Skorobogatov and W. Christopher, “Breakthrough silicon scanning discovers backdoor in military chip,” Springer Berlin Heidelberg, pp. 23-40, 2012.

22. S. T. King, T. Joseph, C. Anthony, and G. Chris, J. Weihang, and Z. Yuanyuan, “Designing and implementing malicious processors,” Wild and Crazy Ideas Session VI (ASPLOS XIII), 2008.

۲۳. قادری، ف، نگاهی به تهدیدات سخت‌افزاری، فصلنامه مرکز تحقیقات صنایع انفورماتیک، ۱۳۹۱.

24. ICS-CERT News, ALERT (ICS-CERT-11-161-01): http://ics-cert.us-cert.gov/alerts/ICS-ALERT-11-161-01, june 10, 2011.

25. ICS-CERT News, ICS-CERT News, Advisory (ICSA-13-213-02): https://ics-cert.us-cert.gov/advisories/ICSA-13-213-02, August 01, 2013.

26. http://ics-cert.us-cert.gov/alerts.

27. http://www.ab.com/programmablecontrol/plc/micrologix1100.

28. http://www.kb.cert.org/vuls/id/144233.

29. American Gas Association, “Cryptographic Protection of SCADA Communications,” Technical Report AGA Report, 2005.

30. IEC approves Wireless HART, “Control Engineering,” vol. 55, no. 10, October 2008.

31. V. M. Igure, S. A. Laughter, and R. D. Williams, “Security issues in SCADA networks,” Computers & Security, Computers & Security, vol. 25, no. 7, pp. 498-506, 2006.

32. M. J. Dworkin, SP 800-38C, Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentialit, National Institute of Standards & Technology, 2004.

33. I. Fovino , A. Carcano , M. Masera, and A. Trombetta, “An experimental investigation of malware attacks on SCADA systems,” International Journal of Critical Infrastructure Protection, vol. 2, no. 4, pp. 139-145, 2009.

34. C. Zimmer , B. Bhat , F. Mueller, and S. Mohan, “Time-based intrusion detection in cyber-physical systems,” Proceedings of the 1st ACM/IEEE International Conference on Cyber-Physical Systems, pp. 109-118, 2010.

35. S. Cheung , B. Dutertre , M. Fong , U. Lindqvist, K. Skinner, and A. Valdes, “Using model-based intrusion detection for SCADA networks,” Proceedings of the SCADA Security Scientific Symposium, vol. 46, pp. 1-12, 2007.

36. I. D. A. Modbus, “Modbus application protocol specification,” North Grafton, Massachusetts www. modbus. org/specs. php, 2004.

37. S. Amin, A. A. Cárdenas, and S. S. Sastry, “Safe and secure networked control systems under denial of service attacks,” Hybrid Systems: Computation and Control, Springer Berlin Heidelberg, pp. 31-45, 2009.

38. I. Modbus, “Modbus Messaging on TCP/IP Implementation Guide,” North Grafton, Massachusetts, www. modbus. org/specs. Php, 2004.

39. S. Raza, A. Slabbert, T. Voigt, and K. Landernas, “Security considerations for the wirelesshart protocol,” IEEE Conference on Technologies & Factory Automation (ETFA), pp. 1-8, 2009.

40. S. Raza, T. Voigt, A. Slabbert, and K. Landernäs, “Design and implementation of a Security Manager for Wireless HART networks,” IEEE 6th International Conference on Mobile Adhoc and Sensor Systems (MASS), pp. 995-1004, 2009.

Comprehensive Conceptual Model of Control System's Vulnerabilities

A. Afshar*

A. Termechi

A. Golshan

A. Aghaeian

H. Shahriari

S. Soleymani

Abstract

Although the use of computer and information technology in Industrial Control Systems (ICSs) has enhanced their quality, performance and reliability, it has exposed them to cyber security issues. On the other hand, each ICS has a layered structure owing to its variety of functions. Hence, ICSs are susceptible to a wide array of vulnerabilities. Vulnerability detection is an essential step in securing ICSs. After that, different countermeasures should be applied to mitigate the vulnerabilities. However, there exists the lack of a suitable classification of ICS security related vulnerabilities. To address the issue, this paper presents a comprehensive conceptual model for ICS's vulnerabilities based on available vulnerability classification in security standards and guidelines and layered structure of ICS. AS a result, optimal security controls can be applied to reduce or eliminate the vulnerabilities via the conceptual model. Consequently, the proposed conceptual model can help to identify ICS's vulnerabilities and entry points of ICS and cyber attacks can be prevented as far as possible.

Key Words: *Control System - Cyber Attack - Vulnerability - Conceptual Model.*

*AmirKabir University of Technology - (aafshar@aut.ac.ir)- Writer-in-Charge