
بسم الله الرحمن الرحیم

دانشگاه صنعت آب و برق (شهید عباسپور)
دانشکده مهندسی برق

پایان‌نامه کارشناسی ارشد (مهندسی برق-کنترل)

عنوان پایان‌نامه
ارزیابی سیستم کنترل نیروگاه سیکل ترکیبی طرح نیام شرکت مپنا (Teleperm-XP)، از نظر آسیب پذیری در مقابل بدافزارهای رایانه‌ای و ارائه راهکارهای مناسب

تحقیق و تدوین:
وهاب حاجی‌حاجی

استاد راهنما:
جناب آقای دکتر محسن منتظری

بهمن ۱۳۹۰

دانشگاه صنعت آب و برق (شهید عباسپور)
دانشکده مهندسی برق

پایان‌نامه کارشناسی ارشد رشته مهندسی برق-کنترل آقای وهاب حاجی حاجی

تحت عنوان

ارزیابی سیستم کنترل نیروگاه سیکل ترکیبی طرح نیام شرکت مپنا (Teleperm-XP)، از نظر آسیب پذیری در مقابل بدافزارهای رایانه‌ای و ارائه راهکارهای مناسب

در تاریخ ۱۳۹۰/۱۱/۳۰ توسط کمیته تخصصی زیر مورد بررسی و تصویب قرار گرفت.

۱- استاد راهنمای پایان‌نامه امضاء

۲- استاد داور داخلی امضاء

۳- استاد داور مدعو امضاء

سرپرست تحصیلات تکمیلی دانشکده امضاء

تشکر و قدردانی

پس از حمد و ستایش درگاه حضرت دوست، بر خود لازم می‌دانم از راهنمایی‌های بی‌دریغ و ارزشمند استاد عزیزم جناب آقای دکتر محسن منتظری کمال تشکر و قدردانی را به عمل آورم. ایشان علاوه بر ایفای نقش استاد راهنما، به عنوان الگوی اخلاق نیز همواره سرمشق بنده بوده‌اند.

به نام خدا

تعهدنامه اصالت اثر:

اینجانب وهاب حاجی حاجی تاکید می‌کنم که مطالب مندرج در این پایان‌نامه، حاصل کار پژوهشی اینجانب می‌باشد و به دستاوردهای پژوهشی دیگران که در این نوشته از آن‌ها استفاده شده است مطابق مقررات ارجاع گردیده است.
این پایان‌نامه قبلاً برای احراز هیچ مدرک هم‌سطح، پایین‌تر و بالاتر ارائه نشده است.
کلیه حقوق مادی و معنوی این اثر متعلق به دانشگاه صنعت آب و برق (شهید عباسپور) می‌باشد.

وهاب حاجی حاجی

تقدیم به

پدر و مادر عزیزتر از جانم

و

خواهر و برادر دوست داشتنی‌ام

فهرست مطالب

فهرست تصاویر و نمودارها

چکیده:

در گذشته سیستم‌های کنترل نیروگاهی هیچ گونه تبادل داده یا اشتراک اطلاعاتی با دیگر سیستم‌ها نداشتند. اما امروزه با توجه به نیازمندی جهت بهبود کارایی، بهینه‌سازی و تصمیم‌گیری‌های سریع تجاری، این گونه سیستم‌های صنعتی جزئی از دنیای "بزرگ به هم متصل" شده‌اند و اطلاعات آنها توسط شبکه‌های داخلی، تجاری و یا حتی اینترنت قابل دست‌یابی می‌باشند. این ارتباط و انتقال داده، راه‌ها و فرصت‌های جدیدی را برای تهدید و حملات خرابکارانه علیه این‌گونه سیستم‌های کنترلی ایجاد نموده است. از طرفی پس از حادثه ۱۱ سپتامبر شرایط امنیتی مورد تحمل، دچار تغییرات شدیدی شده است. لذا امروزه مباحث مربوط به امنیت در شبکه‌های کنترل صنعتی و سایر زیرساخت‌های بحرانی، یکی از بحث‌های مهم و چالش برانگیز دولت‌ها می‌باشد. از طرف دیگر یکی از سیستم‌های کنترل نیروگاه‌های سیکل‌ترکیبی رایج در کشور، سیستم کنترلی Teleperm XP ساخت شرکت زیمنس می‌باشد.

هدف از این پژوهش بیان نمودن دلایل اهمیت امنیت اطلاعات در سیستم‌های کنترل نیروگاه‌های سیکل ترکیبی با تاکید بر روی Teleperm XP، تحلیل و شناخت تمایز میان امنیت این گونه سیستم‌ها با سیستم‌های رایج IT، ارزیابی کمی و کیفی وضعیت امنیت در سیستم کنترلی Teleperm XP، راه‌کارها و سیاست‌های امنیتی موجود جهت بهبود امنیت اطلاعات در این سیستم کنترلی می‌باشد.

به منظور ارائه یک ارزیابی صحیح از وضعیت امنیتی سیستم کنترلی Teleperm XP از یک مدل‌سازی سرویس-گرا- وظیفه‌گرا استفاده شده است. این مدلی که بسیار مناسب سیستم‌های کنترل صنعتی و از جمله سیستم کنترلی Teleperm XP می‌باشد، برای اولین بار و در این پایان‌نامه پیشنهاد شده است. این مدل برخلاف مدل‌های وظیفه‌گرا و یا سرویس‌گرا که به تنهایی نمی‌توانند ارتباط دقیق میان زیر سیستم‌ها، تجهیزات و سرویس‌ها را ارائه نمایند و یا اینکه دارای پیچیدگی بسیار بالا می‌باشند، ضمن داشتن سادگی لازم به خوبی می‌تواند ارتباط میان زیر سیستم‌ها، تجهیزات و سرویس‌ها را نشان دهد. بر اساس این مدل پیشنهادی اقدام به مدل‌سازی سیستم کنترلی و بررسی دقیق ارتباط میان زیرسیستم‌ها، تجهیزات و سرویس‌ها نموده و سپس با شناسایی آسیب‌پذیری‌های سیستم کنترلی و تعریف سناریوهای حمله و با استفاده از درخت حمله اقدام به ارزیابی کمی محاسبه آسیب‌پذیری کل سیستم کنترلی نموده‌ایم. نتایج حاصل از ارزیابی امنیتی سیستم کنترلی Teleperm XP نشان دهنده ضعف امنیتی آشکار در این ساختار کنترلی و عدم به کارگیری تجهیزات و سیاست‌های امنیتی مناسب، می‌باشد. قابل ذکر است که این ارزیابی براساس استانداردهای موجود در حوزه سیستم‌های کنترل صنعتی و برای اولین بار است که بر روی سیستم کنترل نیروگاه سیکل‌ترکیبی، Teleperm XP، موجود در کشور صورت می‌گیرد. در نهایت با توجه به اقدامات امنیتی موجود و با توجه به آسیب‌پذیری‌های شناسایی شده، اقدام به ارائه راه‌کارهای مناسب، جهت اصلاح امنیتی سیستم کنترلی Teleperm XP نموده‌ایم. که بایستی در به کارگیری این سیستم کنترلی مد نظر قرار گیرد.

کلمات کلیدی: سیستم کنترل نیروگاه، سیکل ترکیبی، امنیت اطلاعات، حملات خرابکارانه

فصل اول:
مقدمه

1-1- ضرورت بحث

در گذشته سیستم‌های کنترلی که شامل تمامی سیستم‌های کنترل صنعتی، کنترل فرآیند، کنترل نظارتی (SCADA[1]) و کنترل توزیع شده (DCS[2]) و اتوماتیک می‌باشند، در یک محیط مجزا یا ایزوله شده به کار خود می‌پرداختند و هیچ گونه تبادل داده یا اشتراک اطلاعاتی با دیگر سیستم‌ها نداشتند. این گونه سیستم‌ها دارای یک سخت‌افزار، نرم‌افزار و پروتکل اختصاصی مربوط به خود بوده که جهت پایش و کنترل فرآیندهای حساس طراحی شده بودند. به دلیل محدودیت شدید در دسترسی به اطلاعات این نوع سیستم‌های کنترلی و دانش محدود درباره پروتکل‌های بکارگرفته شده جهت تبادل داده در آنها، تلاش برای برقراری امنیت شبکه‌های کنترل سیستم بسیار کم بوده و تمرکز اصلی روی خود عملیات کنترل بوده است.

امروزه به دلیل نیازمندی به تبادل داده و اطلاعات، جهت تصمیم‌گیری‌های تجاری و مالی سریع، درخواست برای دسترسی به اطلاعات بلادرنگ فرآیندها در هر نقطه و مکانی بسیار زیاد می‌باشد. این نیاز و درخواست باعث شده است تا سیستم‌های کنترل جزئی از دنیای "بزرگ و به هم متصل" شوند، جایی که اطلاعات کنترل بلادرنگ می‌تواند بسادگی توسط مدیران تجاری، مهندسین، متخصصین تعمیر و نگهداری و فروشنده‌ها و البته توسط شبکه‌های تجاری و یا حتی اینترنت مورد استفاده قرار گیرند. این افزایش در ارتباطات خود مستلزم پذیرش و رعایت استانداردها در پروتکل‌ها و تکنولوژی بکارگرفته شده و همچنین سیستم عامل‌های مورد استفاده، می‌باشد.

اکثر سیستم‌های کنترل مدرن امروزی به شدت به سیستم عامل‌های تجاری و استانداردهای باز همانند: اترنت و تکنولوژی وب وابسته می‌باشند. از طرفی دیگر این استانداردها و ابزار ذاتاً برای محیط‌های تجاری توسعه یافته‌اند، در نتیجه این ارتباط و وابستگی باعث به وجود آمدن خطرات و تهدیداتی خواهد شد که در گذشته برای سیستم‌های صنعتی وجود نداشته است.

در سال‌های اخیر جهش زیادی در نیاز به حفظ این گونه تأسیسات صنعتی و کنترلی در مقابل فعالیت‌های تهدید آمیز موجود توسط تروریست‌ها، سازمان‌های جاسوسی یا گروه‌های تندرو بوده است. به عبارت دیگر، شرایط امنیتی مورد تحمل بعد از حملات ۱۱ سپتامبر دچار تغییرات شدیدی شده است. از طرفی دیگر، گسترش استفاده از تکنولوژی ارتباطات و انتقال، راه های جدیدی را برای حملات خرابکارانه باز می‌گذارد.

تجربه Stuxnet خود نشان دهنده تحولی بزرگ در فعالیت‌های تهدیدآمیز موجود برای سیستم‌های کنترل صنعتی را نشان می‌دهد. این بدافزار در اواسط تیرماه ۱۳۸۹ در سراسر جهان انتشار یافت. نخستین بار کارشناسان کامپیوتری بلاروس متوجه وجود ویروسی شدند که هدف آن سامانه‌های هدایت‌گر تأسیسات صنعتی با سیستم عامل

[1] Supervisory Control and Data Acquisition
[2] Distributed Control System

ویندوز می‌باشد. کارشناسان معتقدند طراحان این بدافزار یک منطقه جغرافیایی خاص را مدنظر داشته‌اند. طبق گزارشات منتشر شده توسط متخصصین هدف از طراحی این بدافزار دستیابی به اطلاعات صنعتی ایران می‌باشد. این بدافزار برای جلوگیری از شناسایی شدن خود از امضای دیجیتالی شرکت‌های معتبر استفاده می‌کند .

با توجه به موارد ذکر شده نیاز به حفظ این گونه تأسیسات صنعتی و کنترلی در مقابل فعالیت‌های تهدیدآمیز موجود توسط تروریست‌ها، سازمان‌های جاسوسی یا گروه‌های تندرو بسیار ضروری می‌باشد. به طوری که افراد و گروه‌های مختلفی سعی در ارزیابی و تحلیل آسیب‌پذیری‌های این قبیل سیستم‌های کنترلی در مقابل حملات اطلاعاتی داشته‌اند و اقدام به بررسی و ارزیابی امنیتی سیستم‌های کنترل صنعتی و ارائه راه‌کارهای مناسب برای ارتقاء امنیت اطلاعات در آن، نموده‌اند.

با توجه به اهمیت امنیت اطلاعات در سیستم‌های کنترل صنعتی و از طرفی دیگر، وضعیت کشور نیازمند تحقیق و پژوهش فراوان در این حوزه امنیتی می‌باشیم. ولی متأسفانه به دلیل عدم اطلاع کافی افراد و متخصصین موجود در حوزه صنعت درباره اهمیت امنیت اطلاعات در سیستم‌های کنترل صنعتی و نتایج وخیم حاصل از حملات اطلاعاتی، این حوزه تحقیقاتی و پژوهشی مورد توجه قرار نگرفته است. از طرفی یکی از متداول‌ترین سیستم‌های کنترلی نیروگاه سیکل‌ترکیبی در کشور، سیستم کنترلی Teleperm XP ساخت شرکت زیمنس بوده و همواره تعداد آنها در کشور روبه افزایش می‌باشد. بنابراین با توجه به تهدیدات موجود برای این گونه سیستم‌های کنترل صنعتی و نیروگاهی، شناخت هرچه بیشتر این سیستم‌ها و تحلیل آسیب‌پذیری‌های امنیتی مربوط به آن بسیار ضروری می‌باشد. لذا در این پروژه سعی شده است تا ضمن بررسی ساختار سیستم کنترلی Teleperm XP اقدام به ارزیابی امنیتی، شناسایی آسیب‌پذیری‌ها و تهدیدات احتمالی آن در مقابل حملات اطلاعاتی بنماییم. سپس اقدامات و توصیه‌های امنیتی لازم جهت رفع و یا کاهش آسیب‌پذیری‌های این سیستم کنترلی را ارائه نماییم.

۱-۲- تهدیدات رایج امنیتی

تهدیدات امنیتی به صورت مجموعه‌ای از رویدادها یا وقایع با پتانسیل ایجاد تخریب، فاش نمودن اطلاعات محرمانه، تغییر دادن داده‌ها و یا انکار سرویس، از داخل و خارج سازمان تعریف می‌شوند. تهدیدات داخلی دارای دو منبع اصلی می‌باشند[۱]:

- رویدادهای تصادفی زمانی ایجاد می‌شوند که یک فرد ناآگاه، آموزش ندیده و یا بی‌دقت یک عملیات غیر عمدی را انجام دهند. در اکثر موارد، این گونه حوادث ناشی از سیاست‌ها یا فرآیندهای غلط، تصدیق هویت و محدودیت دسترسی نادرست و یا اشتراک نام کاربری و کلمه عبور، می‌باشند.
- رویدادهای برنامه ریزی شده که توسط، افراد یا گروه‌ها و با یک برنامه‌ریزی و آگاهی کافی از سیستم کنترلی مورد نظر صورت می‌گیرد.

تهدیدات خارجی سیستم‌های کنترلی به صورت زیر طبقه‌بندی می‌شوند:

- نرم‌افزارهای مخرب[1]: تمامی سیستم‌های اطلاعاتی و سیستم‌های کنترلی به طور بالقوه در معرض آسیب-پذیری ناشی از ویروس‌ها، کرم‌ها، تروجان‌ها و نرم‌افزارهای جاسوسی می‌باشند. حملات ناشی از این قبیل تهدیدات می‌تواند باعث مسدود کردن و خرابی مسیر تبادل داده، نصب نرم‌افزارهای خارجی و یا خاموشی اجباری در سیستم‌های کنترل صنعتی شود.
- هکر[2]: افرادی که علاقه‌مند به جست و جو مراکز اطلاعاتی، ایجاد مزاحمت و کنترل سیستم‌ها به منظور ایجاد مشکل و یا کسب شهرت می‌باشند.
- تروریست[3]: این قبیل تهدیدات خارجی، سیستم‌های بحرانی را شناسایی کرده و اطلاعات آنها را به سرقت برده و یا تخریب می‌نمایند. این نوع تهدید خارجی، بزرگ‌ترین نگرانی دولت‌ها می‌باشند.

۱-۳- نتایج حملات امنیتی در سیستم‌های کنترل صنعتی

ارزیابی پیامدها و نتایج حملات اطلاعاتی در محیط‌های صنعتی به سادگی یک برآورد مالی ناشی از یک واقعه نمی‌باشد. برای سیستم‌های کنترل نیروگاهی و تولیدی که اغلب به طور مستقیم به شبکه‌های انتقال و تولید انرژی الکتریکی و فرآیندها متصل شده‌اند وقوع یک رویداد امنیتی می‌تواند نتایج وخیمی از قبیل خطرات امنیت عمومی، زیست محیطی و یا از دست رفتن اطلاعات محرمانه، از دست رفتن محصول و تولید، تخریب تجهیزات و از دست رفتن اعتماد عمومی گردد. این باعث می‌شود تا نتایج یک حمله اطلاعاتی به تجهیزات صنعتی بسیار بیشتر از یک ضرر مالی باشد. اگر چه تأثیرات مستقیم مالی (مانند از دست رفتن تولید و یا خرابی دستگاه) وجود دارد ولی برای اغلب کمپانی‌ها، ضربه وارده به اعتبار و آبروی آنها با اهمیت‌تر از هزینه‌های حاصل از قطع تولید می‌باشد. ضربه به سلامت و اعتبار نشان تجاری یک کمپانی می‌تواند بسیار زیان‌بار باشد. از جمله برخی دیگر از پیامدهای حملات اطلاعاتی به سیستم کنترل نیروگاهی سیکل ترکیبی می‌توان به موارد زیر اشاره نمود:

- عدم دسترسی به منابع، از قبیل شبکه تجاری و یا شبکه کنترل نیروگاهی
- از دست رفتن اختیار تجهیزات و کنترل کننده‌ها

گسترش ویروس به کل سیستم می‌تواند باعث از دست رفتن کنترل HMI و یا تخریب بایگانی فرآیند و یا با ارائه یک تصویر غلط از وضعیت نیروگاه منجر به از دست رفتن کنترل و حتی به خطر افتادن جان افراد گردد.

در نتیجه شدت این نتایج، کاملاً واضح است که تلاش جهت حفاظت سیستم‌های کنترل صنعتی و نیروگاهی بسیار ضروری می‌باشد.

[1] Malware
[2] Hacker
[3] Terrorist