



شرکت توانیر

تشریح پروژه واگذاری

CoRFP20-14



عنوان پروژه: طراحی و ساخت سیستم تشخیص نفوذ مبتنی بر شبکه متناسب با پروتکل IEC60870-5-104

عنوان طرح:

طرح توسعه فناوری های امنیتی در صنعت برق

واحد اجرایی:

مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق

برآورد کلی مدت زمان اجرای پروژه: ۱۰ ماه

تبیین و تشریح پروژه همراه با ذکر مراحل کلی:

تشخیص نفوذ به فرآیند نظارت بر رویدادهایی که در سیستم رایانه یا شبکه رخ می دهند و تجزیه و تحلیل آنها به منظور یافتن مشخصاتی از حوادث محتمل گفته می شود. این حوادث می توانند تجاوزها یا تهدیدات قریب الوقوع برای نقض سیاست های امنیتی رایانه، سیاست های مورد استفاده پذیرفته شده یا شیوه های امنیتی استاندارد باشند. این حوادث ممکن است به دلایل متفاوتی از جمله بدافزارها (مانند کرم ها و ویروس ها)، دسترسی بدون مجوز به سیستم ها توسط مهاجمین از طریق اینترنت و کاربران مجازی که از امتیازاتشان سوء استفاده می کنند یا سعی می کنند امتیازات بیش تری که مجاز به داشتن آنها نیستند را به دست آورند رخ دهند.

سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) با قابلیت پشتیبانی از پروتکل IEC60870-5-104، تجهیز می باشد که بر ارتباطات مراکز دیسپاچینگ و پایانه راه دور تحت این پروتکل نظارت دارد و فعالیت های این پروتکل را با هدف شناسایی فعالیت های مشکوک تحلیل نموده و حملات را شناسایی می کند. NIDS می تواند به روش مبتنی بر امضاء، بر مبنای تحلیل رفتار یا بصورت ترکیبی هر دو روش، پیاده سازی شوند.

پروتکل IEC60870-5-104 یک پروتکل ارتباطی است که در سیستم های اسکادا برای برقراری ارتباط بین مراکز کنترل دیسپاچینگ و تجهیزات و پایانه های راه دور (RTUها) کاربرد دارد.

در این پروژه طراحی یک NIDS برای کاربردهای صنعتی با روش تشخیص نفوذ ترکیبی مورد نظر می باشد که قابلیت ادراک و تحلیل پروتکل صنعتی IEC60870-5-104 را به صورت کامل داشته باشد.

مراحل کلی پیشنهادی برای اجرای این پروژه به شرح زیر می باشد:

- مرحله ی اول - مطالعات اولیه در ارتباط با سیستم های تشخیص نفوذ مبتنی بر شبکه ی صنعتی و پروتکل IEC60870-5-104
- مرحله ی دوم - استخراج الزامات پیاده سازی
- مرحله ی سوم - پیاده سازی اولیه
- مرحله ی چهارم - تست و برطرف سازی اشکالات
- مرحله ی پنجم - پیاده سازی نهایی
- مرحله ششم - ارائه نتایج تست و ارزیابی در آزمایشگاه های مرتبط



شرکت توانیر

تشریح پروژه واکذاری

CoRFP20-14



عنوان پروژه: طراحی و ساخت سیستم تشخیص نفوذ مبتنی بر شبکه متناسب با پروتکل IEC60870-5-104

عنوان طرح: طرح توسعه فناوری های امنیتی در صنعت برق

واحد اجرایی: مرکز توسعه فناوری امنیت اطلاعات، ارتباطات و تجهیزات صنعت برق

برآورد کلی مدت زمان اجرای پروژه: ۱۰ ماه

مشخصات محصول نهایی (خروجی مورد انتظار):

طراحی و تولید نمونه نیمه صنعتی یک سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) با حداقل قابلیت های زیر:

- متناسب و سازگار با پروتکل IEC60870-5-104
- تشخیص نفوذ حملات مشخص توسط امضاء
- استفاده از روش های تحلیلی برای تشخیص نفوذ مبتنی بر رفتار
- پایش شبکه و تشخیص فعالیت های مخرب شامل:
 - بسته های نافرمان بر اثر حمله ی سرریز بافر
 - اتصال دستگاه های مشکوک به شبکه از جمله رسانه های قابل حمل
 - حملات منع سرویس
 - بازپخش پیوسته ی ترافیک کنترلی مشترک در یک حمله ی تکرار
- فراهم آوردن امکانات زیر:
 - پشتیبانی از به روزرسانی امضاها
 - قابلیت دریافت و ثبت اطلاعات مربوط به تنظیمات و کارایی مانند سرعت پورت ها، مسیریابی نامناسب، ترافیک غیر ضروری
 - قابلیت اتصال همتا به همتا از طریق لیست سفید برای مدیریت موثرتر سیستم