	فرم تشریح پروژه	شرکت توانیر
	CoRFP20-4	

عنوان پروژه:	**طراحی و ساخت سیستم تشخیص نفوذ مبتنی بر شبکه متناسب با پروتکل DNP3**
عنوان طرح:	**طرح توسعه فناوری‌های 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 می‌دهند و تجزیه و تحلیل آن‌ها به منظور یافتن مشخصاتی از حوادث محتمل گفته می‌شود. این حوادث می‌توانند تجاوزها یا تهدیدات قریب‌الوقوع برای نقض سیاست‌های امنیتی رایانه، سیاست‌های مورد استفاده پذیرفته شده یا شیوه‌های امنیتی استاندارد باشند. این حوادث ممکن است به دلایل متفاوتی از جمله بدافزارها (مانند کرم‌ها و ویروس‌ها)، دسترسی بدون مجوز به سیستم‌ها توسط مهاجمین از طریق اینترنت و کاربران مجازی که از امتیازاتشان سوءاستفاده می‌کنند یا سعی می‌کنند امتیازات بیش‌تری که مجاز به داشتن آن‌ها نیستند را به دست آورند رخ دهند.

سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) با قابلیت پشتیبانی از پروتکل DNP3 تجهیزی می باشد که بر ارتباطات مراکز دیسپاچینگ و پایانه راه دور تحت این پروتکل نظارت دارد و فعالیت‌های این پروتکل را با هدف شناسایی فعالیت‌های مشکوک تحلیل نموده و حملات را شناسایی می‌کند. NIDS می توانند به روش مبتنی بر امضاء، بر مبنای تحلیل رفتار یا بصورت ترکیبی دو پیاده سازی شوند.

پروتکل DNP3.0 یک پروتکل ارتباطی است که در سیستم‌های 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 DNP3 را به صورت کامل داشته باشند.

مراحل کلی پیشنهادی برای اجرای این پروژه به شرح زیر می‌باشد:

- مرحله‌ی اول – مطالعات اولیه در ارتباط با سیستم‌های تشخیص نفوذ مبتنی بر شبکه‌ی صنعتی و پروتکل DNP3
- مرحله‌ی دوم – استخراج الزامات پیاده‌سازی
- مرحله‌ی سوم – پیاده سازی اولیه
- مرحله‌ی چهارم – تست و برطرف سازی اشکالات
- مرحله‌ی پنجم –پیاده‌سازی نهایی
- مرحله ششم – ارائه نتایج تست و ارزیابی در آزمایشگاه‌های مرتبط

	فرم تشریح پروژه	شرکت توانیر
	CoRFP20-4	

عنوان پروژه:	**طراحی و ساخت سیستم تشخیص نفوذ مبتنی بر شبکه متناسب با پروتکل DNP3**
عنوان طرح:	**طرح توسعه فناوری‌های 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 نیمه صنعتی یک سیستم تشخیص نفوذ مبتنی بر شبکه (NIDS) با حداقل قابلیت های زیر:

- متناسب و سازگار با پروتکل DNP3
- تشخیص نفوذ حملات مشخص توسط امضاء
- استفاده از روش‌های تحلیلی برای تشخیص نفوذ مبتنی بر رفتار

- پایش شبکه و تشخیص فعالیت‌های مخرب شامل:
  - بسته‌های نافرم بر اثر حمله‌ی سرریز بافر
  - اتصال دستگاه‌های مشکوک به شبکه از جمله رسانه‌های قابل حمل
  - حملات منع سرویس
  - بازپخش پیوسته‌ی ترافیک کنترلی مشترک در یک حمله‌ی تکرار
- فراهم آوردن امکانات زیر:
  - پشتیبانی از به‌روزرسانی امضاها
  - قابلیت دریافت و ثبت اطلاعات مربوط به تنظیمات و کارایی مانند سرعت پورت‌ها، مسیریابی نامناسب، ترافیک غیرضروری
  - قابلیت اتصال همتا به همتای مطمئن از طریق لیست سفید برای مدیریت موثرتر سیستم