Descubriendo Controladores Lógicos Programables en una Red Universitaria

Héctor Fabio Jiménez Saldarriaga
Universidad Tecnológica de Pereira,
Ingeniería de Sistemas y Computación,
Pereira Security Team

Sebastian Zapata Ruiz
Universidad Tecnológica de Pereira,
Ingeniería de Sistemas y Computación

El uso de los dispositivos electrónicos como los controladores lógicos programables en el campo de la automatización y el control de procesos tienen un rol importante, estos se implementan en muchos campos, e industrias donde los procesos de producción y administración son complicados, críticos y peligrosos tanto económicamente como para la vida humana. En este artículo evidenciamos cómo es posible realizar el descubrimiento de estos dispositivos en un entorno controlado que presenta múltiples PLC's, Computadores de Monitoreo corriendo bajo sistemas operativos Windows, en un a infraestructura universitaria.

Keywords: Redes Industriales , Seguridad Informática, Controladores Lógicos

Introducción

Los controladores lógicos programables (*Programmable logic controller*, de ahora en adelante PLC) fueron diseños en los años 60s[Ref1, Segovia] cuando el control de las maquinas industriales se hacía mediante el uso de relés como en la figura (1), en ese entonces era tedioso y complicado para un técnico encontrar una falla en el sistema eléctrico de control debido a que todo los procesos se encontraban en cuartos llenos de una gran cantidad de cables y relés, lo que dificultaba la búsqueda. Con la llegada de los PLCs se resolvió el problema de la flexibilidad y solución de problemas comunes; estos reemplazaron decenas de cuartos en pocos, albergando bloques compactos de PLC, con ventajas como fácil mantenimiento, instalación, expansión. Su labor principal es la regulación los actuadores electromecánicos, como pueden ser válvulas, sensores, bombas, motores, etc.

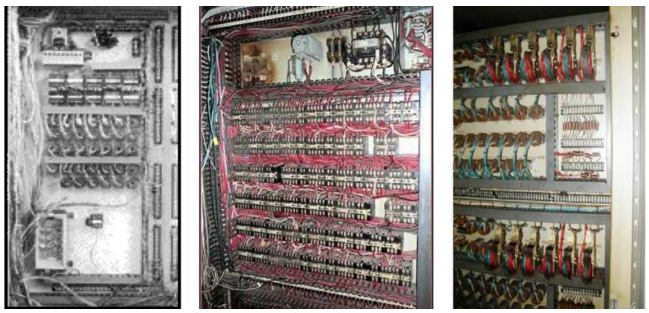

Figura 1. Cuarto de Control Reles, 1974.

Los sistemas de control utilizan como uno de los elementos conformantes a los PLCs para regular procesos industriales ejemplos de estas tareas se ve en lineas de producción de químicos, líneas de ensamble y manufactura, maniobra de maquinaria pesada, control y manejo de señales, control de mezclas, control de generación y despacho eléctrico entre otros(Referencia Porcentajes). En un principio de estos dispositivos se presentaba la situación de que cada PLC actúa como controlador individual e independiente, pero con el crecimiento y demanda de los procesos se requería tener conexiones con otros PLCs, pero funcionando aun así en un contexto local, sin conexiones a redes corporativas o Internet(Ref ENISA, Protecting Industrial Control Systems). En los últimos 15 años con la globalización y la descentralización de las empresas que administran estos procesos se vuelve necesario tener que conectar estos dispositivos mediante enlaces privados e infraestructura pública, sin tener en mente los pilares de la seguridad de la información, confidencialidad, integridad, autenticidad.

Una parte esencial de los sistemas de control industrial (de ahora en adelante SCI) son los sistemas SCADA (*Supervisory Control and Data Acquisition*), responsables de obtener información relevante y basados en el análisis de esta información enviar instrucciones a los sistemas de producción. Los sistemas SCADA necesitan estar conectados en varias niveles topológicos dentro del sistema de control industrial, ejemplo de ello se puede ver en la figura (2).

Sistemas de Control Industrial (SCI)

Un sistema de Control industrial se compone de distintos elementos y zonas como se muestra en la figura(2), los más representativos son :

- Sistema de administración de operaciones
- Gestión de operaciones Comerciales
- Sistema de Control y Adquisición de Datos
- Red de Supervisión
- Sistemas de Proceso y Control . . .

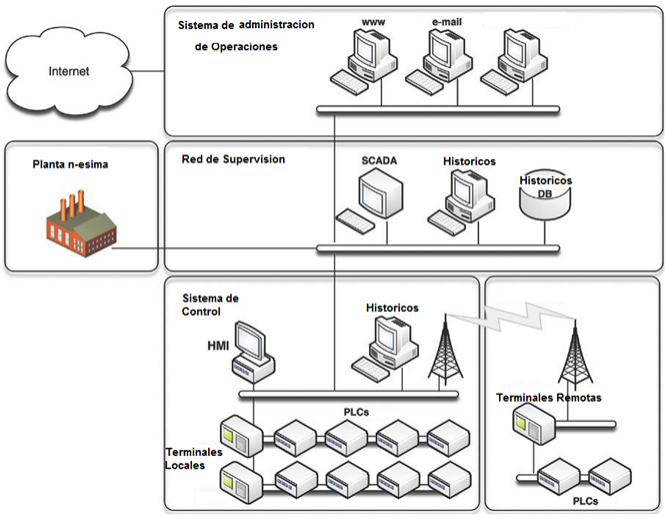

Figura 2. Sistemas de Control Industrial (SCI)

Cada zona o elemento tiene su propio fin físico y lógico, además de las consideraciones de seguridad, y políticas a implementar, se debe de ver que existen dependencias entre los diferentes niveles.

Sistema SCADA y Protocolos

Un sistema SCADA típico consiste de diferentes partes. El algoritmo de control de más bajo nivel se ejecuta en un PLC o terminal remota. Estos dispositivos están conectados a sensores y actuadores. Ellos reciben los datos proporcionados por los sensores, evalúan el estado del sistema local y controlan los actuadores basados en el resultado del análisis de los datos. Los PLC pueden ser conectados en diferentes topologías e integrarse entre sí para ser supervisados y monitoreados por el SCADA como se muestra en la pirámide de automatización Para alcanzar el Sistema de supervisión se requiere de una computadora normal típicamente corriendo alguna versión de software SCADA [ListofScadaRef] que permite realizar diagnósticos remotos, envió de instrucciones o reprogramación de control a los PLCs. Una base de datos de históricos almacena datos de los eventos presentados en el pasado para evaluaciones futuras [RefTrendMicro].

Los SCADA hacen uso de protocolos de redes para el transporte de administración y programación de los comandos del PLC. Los protocolos también se utilizan para la comunicar entre PLCs. La conexión a las redes corporativas y

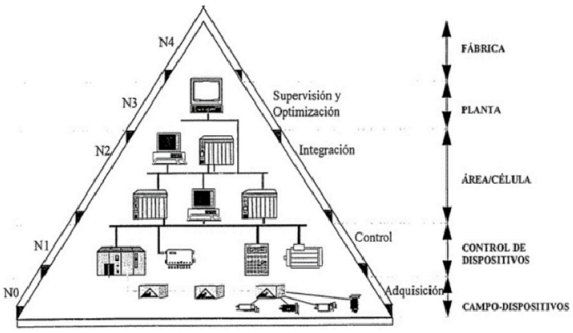

Figura 3. Piramide de Automatización,Niveles.

/ o Internet - por ejemplo, para el mantenimiento remoto - se realiza con frecuencia a través de protocolo estándar, como HTTP, Telnet o FTP. Conectividad en la capa de enlace que por lo general se lleva a cabo a través de Ethernet.

Pero los protocolos mas usados para los sistemas SCADA son DNP3, ICCP (IEC 60870-6), Modbus, OPC (OLE for process control). Cada uno de estos posee distintas características y sistemas de seguridad y cifrado, aun así, cada uno posee diferentes vulnerabilidades a posibles ataques e inclusive algunos de ellos no realizan ninguna comprobación de seguridad.

Problemas Generales de Seguridad en un SCI

Mencionar uno de las preguntas del nuestra investigación entorno a un SCI.

Configuración del Análisis de Seguridad

Para el desarrollo de esta investigación seguiremos una metodología de seguridad como OSSTMM, además las propuestas prácticas de Dale Peterson (Referencia), Robert Graham, Paul Mcmillan, Dan Tencler (Referencia), y por supuesto recomendaciones del equipo de Zmap https://zmap.io/documentation.html#bestpractices).

Es importante aclarar que el posicionamiento que se tomo es interno, con una visibilidad blackbox y adoptando un perfil de usuario normal, sin privilegios, hay que mencionar que nosotros obtuvimos los permisos legales para llevar a cabo esta investigación pues es de mencionar que realizar estas actividades sin el permiso, podría incurrir en algún acto tipificado como delito informático. El proceso se realizó en un entorno controlado (RefEntorno Controlado) que implico solamente el escaneo de algunas subredes de nuestra red universitaria, en la cual nosotros desconocíamos la topología de la red. Se utilizo un computador portátil, y un computador de escritorio ambos corriendo Debian Gnu/Linux, con procesadores Core2Duo, 2xCore I7, 4 y 8 Gb de Ram, con tarjetas 100/1000, dual-port, conectados a la red que tienen acceso normalmente los estudiantes.

En el escaneo de puertos se emplearon las tres herramientas más populares que son:

- Zmap: Desarrollado por un equipo de tres científicos de computación en la universidad de Michigan, ellos son Ph.D Akir Durumeric, Ph.D(c) Eric Wustrow, y J. Alex Halderman, Profesor asistente, el software se encuentra bajo la licencia de Apache Foundations.
- Masscan: Desarrollado por Robert David Graham el escáner de puertos más rápido del momento, de hecho 10 veces más rápido que el primero, pero requiere de un computador con un procesador de 4 núcleos y una tarjeta ethernet dual-port de 10gbs teóricamente puede transmitir 25 millones de paquetes por segundo, licenciado bajo Gnu Gpl v3.
- Nmap: El scanner que más resultados entrego, es una herramienta de código abierto para exploración de red y auditoría de seguridad. Su líder de desarrollo es Fyodor, posee incorporad un motor de Scripting para la ejecución de scripts personalizados, y realización de diversas tareas de descubrimiento, detección de puertos y servicios en la subred.

El escaneo de puertos indica el estado de los puertos de las máquinas, dispositivos conectadas a las redes, detectando y descubriendo si está abierto, cerrado, o protegido por un cortafuegos. La siguiente imagen presenta una topología aproximada, basados en los datos arrojados por las herramientas, y cantidad de saltos mostrados mediante tracer.

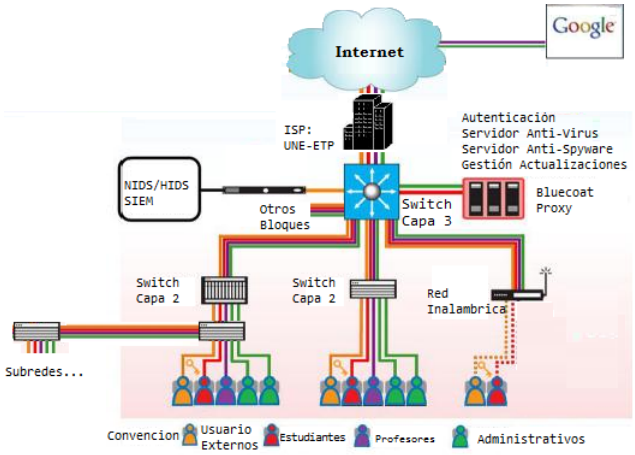

Figura 4. Topologia aproximada, posicionamiento interno.

ADSADASDASD ASDASDASD

Posibles Ataques

Según el protocolo que usen los sistemas SCADA pueden poseer distintas vulnerabilidades, algunos de estos poseen comprobaciones de seguridad, pero aun así las tienen, por

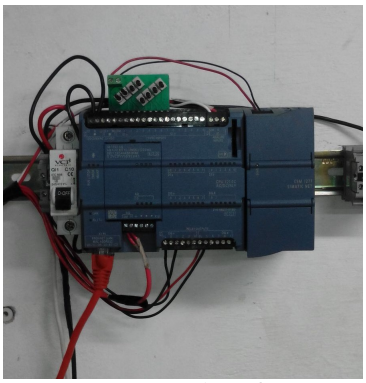

Figura 5. Siemens S7-1200,Red Profinet. Control de Banco Hidraulico.

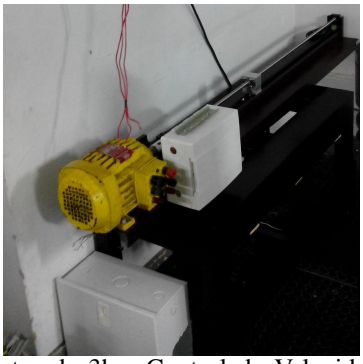

Figura 6. Motor de 3hp, Control de Velocidad posicionamiento de tornillo, practica realizada por estudiantes mediante controladores logicos programables.

ejemplo el protocolo Modbus, cuyo diseño está pensado para operar sobre líneas de transmisión en serie. El modo bajo el cual se da la comunicación de estas redes es un primitivo esquema de "petición-respuesta", que dificulta la identificación de un eventual ataque pues los sistemas no podrían distinguir entre peticiones legítimas o peticiones provenientes de sistemas infectados. El protocolo Modbus está montado sobre TCP y ese protocolo no realiza autenticación ni tiene funcionalidades de confidencialidad de manera nativa, de forma tal que una vez que el hacker logra entrar a la red puede tomar

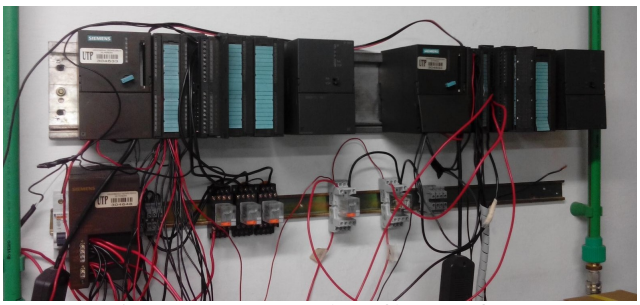

Figura 7. Siemens S7-300, Red Profibus-Profinet

el control de una sesión.

Ataques comunes a las PLC's o también llamados Stuxnet son gusanos que afectan a equipos con Windows, descubierto en junio de 2010 por VirusBlokAda, una empresa de seguridad radicada en Bielorrusia. Es el primer gusano conocido que espía y reprograma sistemas industriales, en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como centrales nucleares. Stuxnet es capaz de reprogramar controladores lógicos programables y ocultar los cambios realizados. Otros posibles ataques a los sistemas SCADA:

- DoS, es un ataque a la denegación de servicios, causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad de la red por el consumo del ancho de banda de la misma.
- Spootfing, el atacante se hace pasar por una entidad distinta a través de la falsificación de los datos en una comunicación.

Resultados

Durante el análisis realizado a las 8192 direcciones IP utilizando los scanerers Zmap[Ref] y nmap [Ref] para correlacionar la información, se utilizo la lista de puertos en los que en los segmentos de los edificios de eléctrica se detectó que no se implementan políticas y reglas adecuadas en los Sistemas de detección de intrusos, se realizaron pruebas básicas de enumeración de usuarios en

Conclusiones

En conclusión, una red SCADA será tan segura como los mecanismos de seguridad que incorporen sus protocolos o puedan aplicarse a los mismos. De nada sirve un firewall si no puede actuar sobre un determinado protocolo; como tampoco querer autenticar o cifrar el intercambio de datos sin la existencia de mecanismos intrínsecos de intercambio de claves.

Organizations should establish workforce behavioral and access baselines, including an understanding of hiring, oversight, access, and security policies, in order to identify anomalies.

Effective prevention and mitigation programs must be driven by better understanding the insider's definition of success against a particular sector

The impacts of a cyberattack that is designed to cause physical damage to critical infrastructure could be much more severe than those of a conventional cyberattack.

Public and private organizations must consider how to balance the best risk-based security procedures against the myriad of policy, legal, and employees' rights issues associated with obtaining and analyzing relevant threat data in the workplace, especially data derived from social media and behavioral monitoring.

http://blog.s21sec.com/2008/12/protocolos-scada-y-seguridad.html Puedes verlo en (?, ?). Te recomiendo leer (?, ?, ?, ?, ?).

Agradecimientos

Los autores desean agradecer a esta universidad, al programa de Ingeniería de Sistemas y Computación y a la profesora Johana Carolina Ochoa por haber asesorado en las consultas y dudas presentadas durante el escrito de este articulo.

Este trabajo de investigación y propuesta experimental fue financiado por los autores, a través del grupo de seguridad informatica Pereira Security Team. También expresar su mayor gratitud con todos aquellos profesores que aportaron y dieron sugerencias, Edison Duque Cardona, al administrador de la red Fabian Franco por su tiempo, Lic. Leidy Tabares Velosa por sus aportes en cuanto a la parte de delitos informaticos, y a todos que nos dieron todos sus comentarios sobre la propuesta.