

INSPIRE, hacia un mundo más seguro



Elyoenai Egozcue
Investigador de Seguridad
S21sec

perspectiva empresarial



Gran parte de las infraestructuras actuales de los países industrializados dependen de lo que hoy en día comienza a ser ya un concepto de moda: los sistemas SCADA. SCADA, que proviene del inglés *Supervisory Control and Data Acquisition* (control de supervisión y adquisición de datos), engloba aquellos dispositivos *hardware* y aplicativos *software* que están detrás del correcto funcionamiento de las centrales de generación de electricidad, de las redes encargadas de su transporte y distribución, de las plantas depuradoras de aguas, de los sistemas de transporte a gran escala, de las refinерías, de los gaseoductos, y otras tantas infraestructuras de carácter crítico para cualquier país.

Estos sistemas han adoptado ya, o se encuentran actualmente en proceso de adoptar, las tecnologías que están detrás, y que sustentan la revolución de Internet: tecnologías estándares, abiertas y escalables, que permiten la interconexión de sistemas a gran escala, la accesibilidad desde cualquier punto del planeta y que garantizan la optimización de costes en las empresas, lo que en definitiva se traduce en una mayor productividad. Este inevitable cambio tecnológico ha empezado a producirse en los últimos años y ha acarreado consigo, además de las ventajas ya citadas, un abanico de nuevas fuentes de amenazas de seguridad hasta ahora no contempladas en este ámbito: piratas informáticos, código malicioso, mafias organizadas, espionaje industrial, guerra cibernética, etc.

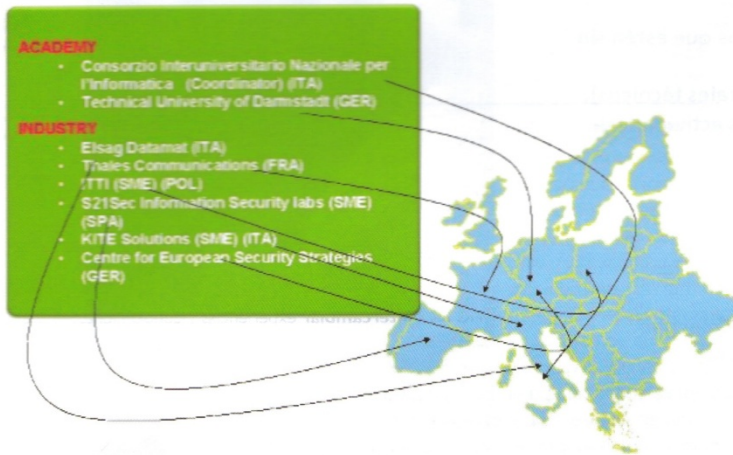
Con el objetivo de hacer frente a esta nueva problemática de

seguridad, surge el proyecto INSPIRE (*INcreasing Security and Protection through Infrastructure Resilience*). Se trata de un proyecto dentro del ámbito del Séptimo Programa Marco, financiado por la Unión Europea y en el que participan ocho organizaciones del ámbito académico y empresarial: Consorzio Interuniversitario Nazionale per l'Informatica (CINI), Technische Universität Darmstadt, Elsag Datamat, Thales, Kite Solutions, Centre for European Security Strategies (CESS), ITTI y, en España, S21sec.

Los principales objetivos de este proyecto de investigación son:

1. Estudiar y desarrollar herramientas para la identificación y posterior modelado de sistemas SCADA, tanto a nivel de topología como de vulnerabilidades asociadas a cada componente, basadas en ontologías y herramientas de inventariado.
2. Desarrollar un *framework* de ayuda a la toma de decisiones para operadores, basado en la información de seguridad proporcionada por el modelo anterior, y en base a reglas expertas parametrizables incluidas en un motor de inferencia.





3. Diseñar e implementar algoritmos de ingeniería de tráfico MPLS y explotar las bondades de la tecnología P2P a través de la definición de una arquitectura de red reconfigurable. La meta es que la red de comunicación en la que se apoye el sistema SCADA pueda garantizar los parámetros de calidad de servicio necesarios para su correcto funcionamiento ante un incidente de seguridad.

4. Desarrollar técnicas de detección y diagnóstico de incidentes de seguridad y estrategias de recuperación que se apoyen en la arquitectura reconfigurable antes mencionada.

Desde España se participa en el desarrollo de un *framework* de diagnóstico de seguridad en entornos SCADA basado en los nuevos estándares de evaluación de la seguridad SCAP (*Security Content Automation Protocol*). Estas tareas refuerzan las investigaciones que se

están realizando en las áreas de auditoría y consultoría técnica. En concreto, se ha potenciado el servicio de auditorías de sistemas SCADA, al poder contar con una herramienta con el que automatizar, y en definitiva agilizar y profesionalizar, las auditorías de seguridad en este tipo de entornos críticos.

Los servicios de consultoría para infraestructuras críticas también han dado un salto cualitativo, incluyendo el conocimiento y la experiencia de seguridad en este tipo de infraestructuras para los usuarios en diferentes aspectos: recomendación de buenas prácticas de seguridad; análisis de seguridad de la red de cliente; diseño de nuevas arquitecturas de red, seguimiento las recomendaciones

propuestas por las principales agencias reguladoras del sector; securización de plataformas; etc.

INSPIRE se encuentra ahora en su segundo y ya último año de vida. Llegado a este grado de madurez, y con el fin de ir más allá de los objetivos inicialmente planteados y de estar a la vanguardia de la investigación en seguridad SCADA, el consorcio ha llegado a un acuerdo de colaboración con el proyecto GridStat de la *Washington State University*. Este proyecto, financiado por el Gobierno estadounidense, se centra en el análisis de las actuales limitaciones de la red eléctrica norteamericana a la hora de afrontar fallos accidentales o ataques físicos o cibernéticos. Actualmente el proyecto se encuentra en la fase de diseño de un marco para el desarrollo de un *middleware* que permita superar estas limitaciones, mediante la diseminación de información de estado, decisiones de control y comandos a lo largo y ancho de extensas áreas de la red eléctrica.

El principal beneficio de este acuerdo de colaboración es que el consorcio, va a tener acceso a datos reales de la red eléctrica norteamericana. Estos datos incluyen modelos de red (topologías, nodos, enlaces, sensores/actuadores, tráfico, etc.), modelos de aplicación (medición, monitorización, etc.), modelos de requisitos (fiabilidad, tiempos de respuesta, etc.) y modelos de perturbación (patrones de ataques y fallos). Todos estos datos serán útiles para dar una dimensión realista y específica a las técnicas y soluciones desarrolladas dentro de INSPIRE. ●