C. Alcaraz, et al., "Gestión segura de redes SCADA", *Nuevas tendencias en gestión de redes, Novática*, pp. 20-25, 2008.
NICS Lab. Publications: https://www.nics.uma.es/publications

Gestión Segura de Redes SCADA

Cristina Alcaraz, Gerardo Fernández, Rodrigo Román, Ángel Balastegui, Javier López

Departamento de Lenguajes y Ciencias de la Computación, Universidad de Málaga

{alcaraz, gerardo, roman, balastegui, jlm}@lcc.uma.es

Resumen

En el momento que se introduce en el mercado nuevas tecnologías basadas en entornos distribuidos comienzan a surgir en paralelo nuevos problemas de seguridad en los sistemas SCADA (*Supervisory Control and Data Acquisition*), los cuales monitorizan y gestionan otras infraestructuras de gran complejidad y escala. Un fallo o una interrupción en uno de sus componentes podría suponer un impacto negativo sobre la funcionalidad de otras infraestructuras, por lo que se hace necesario realizar frecuentes análisis de seguridad para así mantener actualizado el conocimiento y proveer recomendaciones y/o soluciones para mitigar o evitar futuras ocurrencias, garantizando una gestión de red fiable y siempre disponible.

Palabras claves

Gestión de red SCADA, Supervisory Control and Data Acquisition Systems, Análisis de Seguridad.

1.- Introducción

Un sistema SCADA es un sistema complejo cuyo objetivo principal es el de llevar a cabo los procesos de supervisión y gestión de otros sistemas complejos, cuyos recursos son considerados críticos (por ejemplo, el agua, gas, gasóleo o la electricidad). Estos sistemas de control han ido evolucionando con el paso de la historia, estando actualmente basados en entornos distribuidos y con componentes (hardware y software) muy variados, siendo la mayoría de ellos componentes COTS (*Commercial-Off-The-Shelf*) para reducir costes de implementación y mantenimiento.

Esta mezcla e interacción de componentes, junto con la apertura de sus conexiones hacia redes externas como Internet, podría conllevar multitud de problemas de vulnerabilidad en estos sistemas críticos. Además, un fallo o interrupción en alguno de sus componentes podría suponer un impacto importante sobre la continuidad de otras infraestructuras, pudiendo incluso repercutir económicamente a una región, a una nación o naciones [1].

Todos estos problemas obligan al sector industrial a colaborar con la comunidad científica y diversas instituciones. Actualmente, existen varios documentos técnicos y artículos científicos que tratan muchos de estos aspectos [2][3][4]. Sin embargo, y debido al carácter crítico de estos sistemas de control, se hace prácticamente necesario mantener siempre actualizados los procedimientos técnicos-científicos, políticas y estándares, donde se detalle en profundidad nuevas vulnerabilidades y soluciones, y en su caso prever ocurrencias y alternativas futuras. De hecho, este artículo muestra un profundo análisis de seguridad en los puntos de control y accesos al sistema (tanto físico como lógico), proveyendo una visualización reciente de nuevos problemas junto con sus recomendaciones para mejorar la disponibilidad y gestión de una red SCADA.

2.- Arquitectura de un sistema SCADA y problemas

Un sistema SCADA está compuesto por dos tipos de redes básicas (ver figura 1): la red corporativa y la red de control. En la red corporativa, las operaciones están más relacionadas con la supervisión general del sistema y cuyos empleados requieren de procedimientos de autentificación fuerte para interactuar con las bases de datos (históricos, alarmas, etc.) y servidores críticos del sistema. En cambio, en la red de control se proceden a realizar todas aquellas tareas relacionadas con la supervisión, como por ejemplo, abrir/cerrar bomba o solicitar la lectura de un dato. Tales tareas son gestionadas por un IHM (Interfaz Humano Máquina) localizado en el centro principal de control SCADA o subestaciones, y transmitidas a un dispositivo de campo localizado físicamente en la propia planta industrial o en alguna subestación remota. Estos dispositivos, como por ejemplo la RTU (Remote Terminal Unit), se caracteriza por sus capacidades limitadas, su autonomía e independencia para procesar datos e identificar de entre un conjunto de sensores o actuadores cuál es el responsable de la ejecución de la orden. Además, son capaces de establecer comunicaciones con otras subestaciones, con otras RTUs y con otros dispositivos de campo, como por ejemplo una PLC (Programmable Logic Controller). Pueden soportar múltiples sesiones con TCP/IP, y por lo tanto, podrían simultáneamente procesar y responder a varios mensajes provenientes de múltiples fuentes, e igualmente, una misma fuente podría entablar conexión con varias RTUs. Para el control remoto, son capaces de interpretar protocolos específicos, como pueden ser Modbus/TCP [5] o DNP3.0 [6], y algunas RTUs manejan Linux/Unix o Microsoft Windows para dar soporte a aplicaciones Web, y así proveer mediante interfaces gráficas informes a los operarios.

Para gestionar estas remotas desde cualquier punto de localización física es necesario utilizar infraestructuras de comunicación muy versátiles, desde una red Ethernet o una línea de teléfono hasta el uso de Satélite, Microondas, fibra óptica, WiFi, WiMAX, etc., e incluso, algunos sistemas SCADA podrían proveer servicios Web y móviles (GSM o TETRA) para reducir las tareas de mantenimiento y maximizar los costes de operación.

Además, en estos sistemas de control pueden convivir multitud de protocolos propios de automatización industrial basados en TCP/IP para el control remoto, tales como: Modbus/TCP, DNP3.0, ICCP [7], o todos aquellos pertenecientes a la familia de Common Industrial Protocol (CIP), mantenido por *Open DeviceNet Vendors Association* (ODVA) [8], como Ethernet/IP, DeviceNet, CompoNet y ControlNet. No obstante, la mayoría de ellos presentan altas vulnerabilidades al carecer de mecanismos de seguridad.

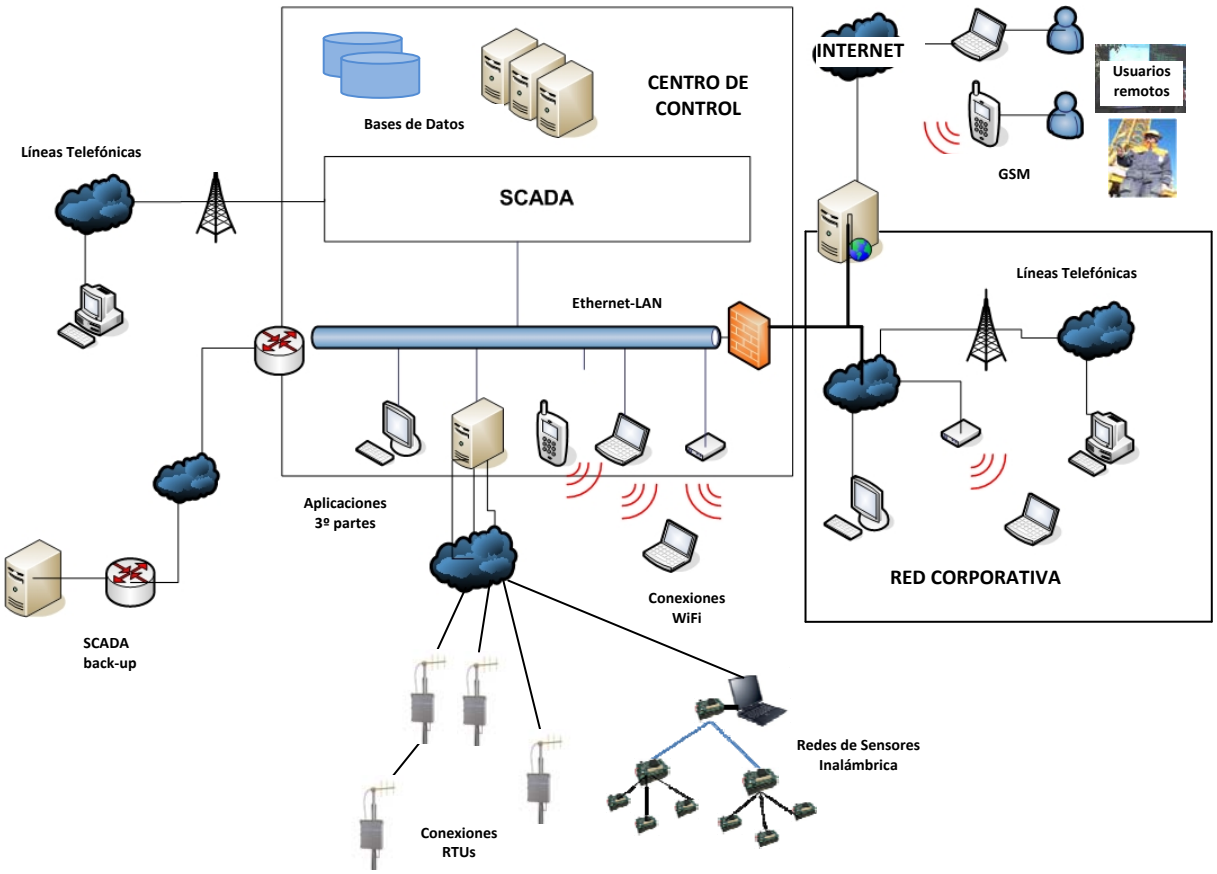

Figura 1: Arquitectura de un sistema de red SCADA

Obviamente, esta arquitectura presenta un riesgo importante desde el punto de vista de la seguridad y disponibilidad del sistema, ya que no sólo suman los diversos ataques conocidos cuando el sistema era cerrado, sino que también se le suman todos aquellos asociados con el estándar TCP/IP y el uso de nuevas tecnologías (por ejemplo, RFID o Redes de Sensores inalámbricas), incluyendo además, todos aquellos problemas de vulnerabilidades asociados con los COTS [9]. Muchas de estas debilidades están registradas en bases de datos públicas, como es el caso de CERT [10], el cual tiene publicado desde 1998 alrededor de 2.500 vulnerabilidades y 150 informes técnicos de seguridad, o el BCIT (*British Columbia Institute of Technology*) [11] con ISID (*Industrial Security Incidents Data*). De hecho, ISID permitió a Byres et.al. [12] concluir que el índice de vulnerabilidades desde el año 2001 eran la mayoría causadas por amenazas externas.

3.- Identificación y autorización en Sistemas SCADA

Para establecer un perímetro de seguridad entre personal no autorizado y cada uno de los componentes e instalaciones críticas de un sistema SCADA es necesario definir e implantar una política de control de acceso fuerte. Esta política debe tener asociado un conjunto de mecanismos adicionales de seguridad que comprenda al menos el uso de dispositivos eléctricos asociados a un computador, como por ejemplo, sistemas biométricos, tarjetas magnéticas, smart cards, RFID, cámara de videos, o incluso, software especializado en realizar los procesos de gestión de identificación y autorización desde un IHM. En caso de que estos sistemas dejen de funcionar, se

aconseja tener como segunda alternativa algún tipo de procedimiento manual para realizar los controles provisionales. El hecho de que se tiendan a diseñar arquitecturas complejas y automatizadas es debido a que estos procedimientos manuales tienen la característica especial de que presentan problemas de seguridad al depender de mecanismos no confiables como una simple llave (tal vez electrónica) o listas de control gestionadas por un ser humano

Hoy en día, la gran mayoría de los sistemas SCADA están basados principalmente en mecanismos de autentificación automatizados basado en usuario/contraseña. La asignación de cuentas dependerán de dos factores importantes, como son: el área de responsabilidad junto con permisos y privilegios asignados a un operador, y el tiempo de actividad según lo prefijado en su contrato. Para el control de cuentas activas como inactivas (tanto por expiración como por baja de contrato), el sistema deberá ejecutar frecuentemente un procedimiento de análisis para comprobar en términos de tiempo la validez de las credenciales de seguridad, y cualquier cambio asociado al usuario deberá ser registrado. Asimismo, cualquier tipo de actividad en una sesión debe ser igualmente registrada para facilitar posteriores procesos de análisis (por ejemplo, estadísticos o forenses). Las credenciales de seguridad deberán estar frecuentemente actualizadas siguiendo unos patrones y una política de control de accesos fuerte. El sistema deberá bloquear todas aquellas cuentas que sobrepasen un cierto umbral de intentos fallidos, limitar el número de sesiones por usuario, y evitar el envío de credenciales de seguridad en claro usando mecanismos criptográficos

Además, muchos de los sistemas SCADA tienden a utilizar en sus arquitecturas servicios Web no sólo para acceder al sistema desde Internet sino para realizar operaciones de control (recibir datos de campo o enviar órdenes de control) en tiempo real desde cualquier IHM. Generalmente, estas páginas web interactúan con las bases de datos relacionales para realizar los procesos de autorización. En caso extremo de que estos servicios web presenten deficiencias de seguridad, existe la posibilidad de que las bases de datos se vean comprometidas. Por lo tanto, se hace casi inevitable adoptar técnicas de desarrollos que prevengan futuros ataques, haciendo uso de herramientas de filtrado que elimine diversos errores de implementación, como por ejemplo DEADBOLT para códigos escritos en C y C++ [13].

No obstante, puede existir un riesgo añadido, y es que habiéndose adoptado las medidas de seguridad comentadas anteriormente, el sistema podría verse comprometido por ataques de ingeniería social o por fuerza bruta. Por lo tanto, es importante definir una política de seguridad adecuada.

4.- Políticas de Seguridad en Sistemas SCADA

Dentro de los sistemas SCADA, es esencial definir una serie de políticas de seguridad. Las políticas de seguridad trasladan los requerimientos de seguridad y fiabilidad de cada sistema SCADA particular a una serie de procedimientos auditable, los cuales permiten salvaguardar la seguridad en su diseño, implementación, y posterior funcionamiento. El alcance de las políticas de seguridad es muy amplio: éstas definen qué acciones pueden o no pueden ser realizadas por los diversos elementos físicos (por ejemplo, los operarios) y lógicos (por ejemplo, el subsistema de comunicaciones), los pasos a seguir durante las operaciones de mantenimiento y gestión de incidencias, además de la cadena

de mando y las responsabilidades de cada uno de los miembros de la organización con respecto a la seguridad del sistema.

A la hora de desarrollar políticas de seguridad para sistemas SCADA, es recomendable seguir las normativas que contemplen controles de seguridad genéricos para sistemas de información. Entre otras, se encuentran las normas NIST 800-53 [14], ISO/IEC 17799 [15], y COBIT [16]. No obstante, los requerimientos específicos de los sistemas SCADA, tales como una alta disponibilidad, fiabilidad, y tiempo de reacción, requieren de un conjunto de normas y políticas adaptadas especialmente a sus necesidades [9]. Con este fin, se han extendido normas existentes [14], desarrollando normas como la NIST 800-82 [17], y definiendo diversos esquemas de políticas de seguridad dentro del ámbito académico [18].

Para cada sistema SCADA, hay que tener en cuenta principalmente las siguientes políticas de seguridad [18]: protección de datos (acceso y almacenaje), configuración del hardware y software (virus, detección de intrusos, control de acceso, cifrado), seguridad en las comunicaciones (acceso inalámbrico, local, remoto), recursos humanos (uso del sistema, preparación y reciclaje), auditorías, seguridad física (acceso a equipamiento, destrucción de material), y ejecución de operaciones de forma manual en caso de fallo. Todas estas políticas de seguridad están influenciadas por los siguientes factores: las interdependencias existentes dentro de la organización, los roles de los diversos recursos humanos, la arquitectura del sistema de información, los datos manejados dentro de SCADA, y los riesgos asociados al sistema.

Como ejemplo de dichas políticas, es posible mencionar las políticas de gestión de incidencias. Un sistema SCADA debe recuperar su funcionamiento lo antes posible ante situaciones anómalas. Por lo tanto, hay que definir tanto el almacenamiento como el acceso a los eventos ocurridos dentro del sistema. También hay que controlar la visibilidad de dichos eventos, así como forzar que operarios con suficientes privilegios conozcan de su existencia. Estos operarios deben disponer de suficiente información (número de teléfonos, correo, claves de cifrado e instrucciones para verificar su identidad) con el fin de contactar con los encargados de la respuesta frente a incidentes. Finalmente, junto con procedimientos de recuperación y puesta en marcha, deben existir accesorios para recopilar y analizar pruebas de evidencias, las cuales pueden preservarse en previsión de posibles acciones legales.

5.- Protección de las Redes de Comunicación SCADA

Para llevar a cabo procesos de gestión de una red SCADA segura será necesario previamente identificar y gestionar todas aquellas conexiones abiertas y directas desde Internet hacia y desde la red SCADA, y desde la red corporativa hacia la red de control mediante mecanismos especializados y restrictivos, tales como: firewalls, IDS (Intrusion Detection System), IPS (Intrusion Prevention Systems), antivirus, servidores RADIUS o protocolos VPN (Virtual Private Networks). Cada uno de estos componentes deberá estar bien configurado y distribuido estratégicamente por todo el sistema con el fin de alcanzar una protección fuerte, y garantizar una defensa en profundidad [19]. Además, será necesario controlar los accesos desde la red corporativa hacia la red de control y hacia diversos servidores críticos, e igualmente, se deberá proteger los enlaces de comunicaciones mediante túneles cifrados, sistemas de gestión

de claves y/o mediante herramientas específicas, como por ejemplo, SecSS (Security Services Suite) [20].

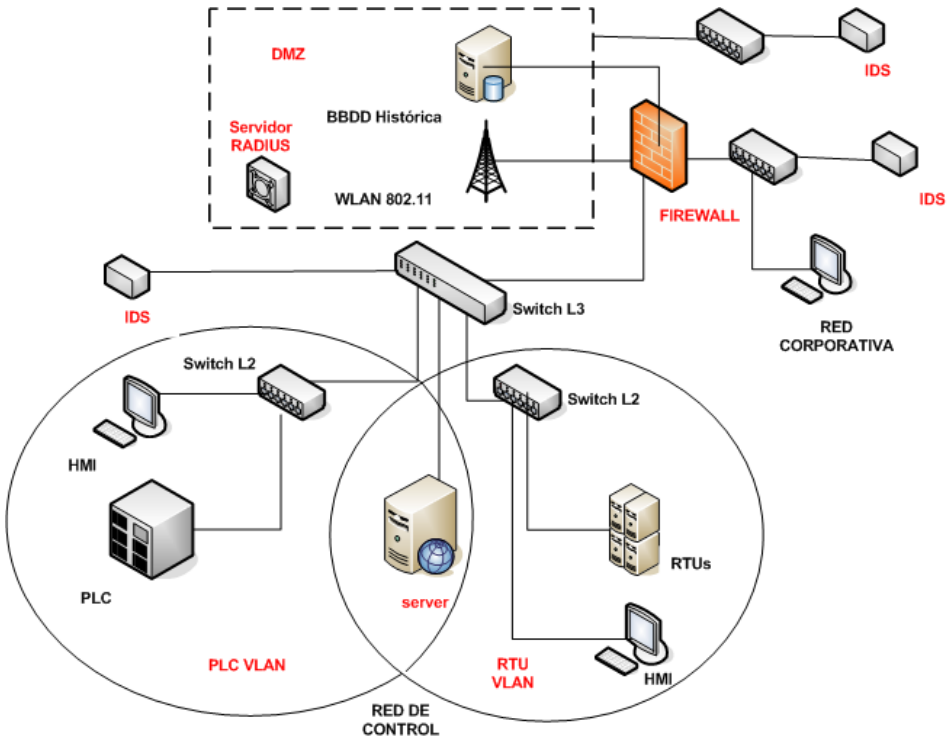

Figura 2: Arquitectura de red SCADA propuesta por NISCC

En el caso de que una parte del sistema está basada en una comunicación inalámbrica (por ejemplo, dispositivos de bluetooth, Rogue APs o WiFi), la política de control de acceso debe ser restrictiva y fuerte. Los puertos inactivos y el broadcast del SSID (Service Set IDentifier) deberán estar desactivados, y se debe hacer uso de mecanismos criptográficos. Es recomendable en estos escenarios el empleo de WPA-Radius y TLS. Por último, dentro de esta categoría, hay que destacar también el papel de las Redes de Sensores Inalámbricas en los procesos de control, ya que esta tecnología es considerada en el presente como una perfecta candidata en la protección de Infraestructuras Críticas en general [21]. Actualmente existen varias iniciativas [22][23] para estandarizar sus comunicaciones en los procesos de control industrial.

5.1.- Primera línea de defensa

En el año 2005, el *National Infrastructure Security Co-ordination Centre* (NISCC) [24] del BCIT presentó una guía para la configuración y gestión de firewalls para sistemas de control. Dicha guía describe una posible arquitectura de red segura y escalable basada en una división de tres zonas principales (ver figura 2), con el objetivo de delimitar cada una de las entidades del sistema, siendo la primera línea de defensa el firewall, los IDS y la DMZ (Demilitarized Zone).

El firewall deberá filtrar, por un lado, direcciones de red, de forma que cada componente SCADA tendrá asignada una dirección IP y uno (o varios) puertos TCP/UDP, y por otro lado, filtrar también a nivel de aplicación, centrando su uso en aquellos servicios de mayor riesgo en una red SCADA, considerando además algunos propios de SCADA. Actualmente, existen varios firewalls exclusivos para entornos industriales, como por ejemplo MODBUS-aware [25] desarrollado por *Cisco Systems*

Critical Infrastructure Assurance Group (CIAG) para Modbus, o Vattenfall [26] para la familia IEC 60870-5 (101, 103 y 104) [27]. También, el NISCC propuso dentro de esta guía el desarrollo de firewalls embebidos en cada uno de los dispositivos de campo, conocidos con el nombre de micro-firewalls. Obviamente, hay que seguir investigando, ya que en general las RTU y PLC carecen de suficiente capacidades computacionales como para analizar continuamente el tráfico entrante y saliente.

Con respecto a los IDS, éstos son los encargados de monitorizar el tráfico de red basándose en patrones y reglas definidas en base a un conocimiento previo de vulnerabilidades y ataques. Esta tarea no es fácil de mantener en un sistema SCADA, ya que se requiere de una persistente actualización de dicho conocimiento. Actualmente, existen algunas herramientas IDS para entornos críticos como [28][29][30], y cualquier tipo de incidencia detectada por éstos deberá ser registrado para realizar, en caso que se requiera, investigaciones forenses.

Finalmente, es importante mencionar que las reglas configuradas en los firewalls no siempre son correctas debido a una incorrecta configuración inicial o por cambios automáticos realizados por los IPS. Una posible solución sería mantener en el sistema una herramienta capaz de analizar en tiempo real, si dichas reglas coinciden con lo establecido en la política de seguridad, como por ejemplo la herramienta APT (Access Policy Tool) [31] desarrollada por la Universidad de Illinois.

5.2.- Protección en los canales de comunicación

Para garantizar disponibilidad y mantenimiento en los sistemas SCADA, las operaciones de control deben ser gestionadas desde cualquier punto de conexión y localización geográfica. Independientemente del tipo de red, los procesos de encriptación deben ser fuertes y los procesos de autentificación restrictivos, y en el caso de que la red de control tenga conexión directa a Internet implementar una VPN basada en SSL dentro de otra basada en IPsec.

Cuando las operaciones de control deben llegar hacia los dispositivos de campo, se hace uso de protocolos específicos como Modbus o DNP3, los cuales carecen de mecanismos de seguridad. Si la comunicación es en serie, el sistema deberá tener instalado un dispositivo mediador entre el puerto EIA-232 de la RTU y el modem para gestionar las operaciones de encriptación de forma transparente. Este dispositivo es conocido con el nombre de Bump-in-the-Wire [32]. Por el contrario, si la comunicación se realiza bajo el estándar TCP/IP, sólo será necesario instalar y configurar aquellos mecanismos de seguridad asociados al estándar.

Igualmente, cuando el tráfico de control proviene de otro centro de telecontrol, éste hace uso del protocolo ICCP/TASE 2.0, el cual provee alta disponibilidad y rendimiento en la transmisión de datos, pero carece también de mecanismos de seguridad. Esto obliga que su diseño esté definido bajo el estándar IEC-62351 del TC57 [33], el cual incluye los protocolos TLS/SSL (para maximizar la interoperabilidad entre sistemas SCADA), MMS/IEC-62351-4 y una tabla bilateral para registrar los enlaces asociados. Todos estos protocolos proveerán al sistema de un soporte para la gestión de certificados, código de autentificación de mensajes, renegociación de cifrados, intercambio de claves de al menos 1024 bits, y firma digital con RSA y DSS, además de habilitar el puerto TCP 3782 para establecer comunicaciones seguras.

Por último, la criptografía y los sistemas de gestión de claves podrían resolver muchos de los problemas de seguridad en los canales de comunicación. Sin embargo, esto no es relativamente fácil de conseguir, ya que existen múltiples e importantes limitaciones asociadas a las capacidades computaciones y de transmisión de datos de los dispositivos de campo. Uno de los primeros informes que agrupó un conjunto de estándares para la implementación de criptografía en fue desarrollado por *American Gas Association* (AGA) con AGA-12 Part 1 [34]. Más tarde, presentaron el AGA-12 Part 2 [35] para describir una técnica de implementación criptográfica en canales de comunicación en serie, incluyendo un protocolo basado en sesiones con servicios de autentificación mediante claves simétricas generadas por AES y SHA-1, y quedan aún pendientes AGA-12 Part 3 y Part 4, donde especifican la protección de los sistemas de redes y la seguridad de dispositivos embebidos en componentes SCADA.

Este mismo grupo de trabajo también estuvo involucrado en desarrollar estándares para la gestión de claves en sistemas de control, y actualmente existen varios grupos de trabajo que están poniéndolo en práctica, como *TC57WG15* (IEC62351), *IEEE Power Engineering Society Substations Committee* con P1689 y *DNP3 User Group* (DNP3 v1.0). Actualmente, existen varias técnicas propuestas, como por ejemplo, hacer uso de Criptografía de Clave Elíptica [36], y es necesario aplicar una metodología de selección [37] apropiada según el tipo de red SCADA diseñado.

6.- Protección de los Sistemas Informáticos

Abordaremos en esta ocasión aquellos procesos orientados a fortalecer la seguridad de los sistemas informáticos encargados de prestar servicios en una red SCADA con el objetivo de frenar o paliar los ataques que puedan realizarse contra ellos.

El año 2008 ha sido prolífico en lo referente a la difusión de ataques realizados sobre sistemas SCADA [38], siendo un factor importante a tener en cuenta el hecho de que aplicaciones de automatización de ataques, como Metasploit, incluyan soporte para atacarlos [39]. Es muy posible que, debido a la notoriedad alcanzada por sus deficiencias en seguridad, los sistemas SCADA supongan un nuevo caldo de cultivo para aquellos deseosos de demostrar sus habilidades.

La adopción de medidas de protección frente a ataques proporciona un grado de seguridad y control extra frente a ataques internos, posiblemente los más peligrosos debido al conocimiento especializado del sistema que posee el atacante. Pero además, suponen una excelente base para afrontar los ataques externos, debido a que construyen un escenario en el que poder controlar el impacto ocasionado por una intrusión.

Una parte fundamental en este proceso consiste en especificar con detalle la dependencia de los servicios implicados con el resto de servicios y/o aplicaciones instaladas. De forma que se puedan diseñar entornos aislados de ejecución para los servicios implicados disminuyendo así la visibilidad y controlando con mayor granularidad los permisos y capacidades de estos servicios con el resto del sistema. Soluciones que implementan este tipo de técnicas están disponibles para los Sistemas Operativos comúnmente empleados en redes SCADA: políticas de grupo y reglas de control de accesos en sistemas Windows, SELinux en Linux (entre otros), RBAC y Contenedores en Solaris. Por consiguiente, y en vistas de facilitar la tarea anterior, será conveniente reducir el número de servicios disponibles en un sistema al mínimo

conjunto necesario, de forma que se disminuyan las dependencias entre servicios y se reduzcan las posibles vías vulnerables al sistema.

El almacenamiento de los datos constituye otro aspecto a tener en cuenta y en muchas situaciones supone la posibilidad para un atacante de escalar privilegios tras una intrusión. Por ello es conveniente adoptar mecanismos de cifrado de datos para aquella información sensible que pueda aumentar el impacto de un ataque. En este grupo podemos incluir también a los servidores de Base de Datos que, tras una valoración del impacto en el rendimiento, deberán habilitar los mecanismos de cifrado de datos para dificultar el que un atacante pueda acceder a los archivos de la Base de Datos en claro.

La monitorización de recursos proporciona un mecanismo que puede ayudar a detectar un comportamiento anómalo o prever un posible fallo del sistema ocasionado por una intrusión. Una sobrecarga injustificada del procesador, un incremento anómalo del tráfico de red y la disminución drástica de la memoria libre o del espacio de disco disponible pueden ser síntomas, entre otros, de que el sistema está siendo atacado o bien se está empleando para atacar otros sistemas. Además, es conveniente emplear soluciones de auditoría de sistemas en los equipos pertenecientes a la red SCADA. De esta forma es posible rastrear las acciones realizadas en un equipo para descubrir tantas evidencias de ataques cómo el alcance de estos ataques en su entorno.

Los sistemas HIDS (Host Intrusion Detection Systems) permiten detectar y frenar ataques comunes mediante técnicas basadas en detección de comportamiento anómalo. Posibilitan que una nueva aplicación instalada por un atacante no pueda ejecutarse, que el software de captura de información que pretende usar el atacante no tenga éxito, la prohibición de acceso físico a memoria o a disco, la protección de controladores sensibles de ataques, etc. La conveniencia de su utilización en un sistema SCADA debe evaluarse con detenimiento, puesto que algunas de las características que proporcionan pueden perjudicar el rendimiento de algunas de las funcionalidades más exigentes de estos sistemas. Como norma general, la mayoría de estas soluciones incluyen un modo de aprendizaje inicial en el cual se crea una configuración de las aplicaciones y comportamientos lícitos para elaborar las reglas de autorización de forma automática. Una vez aprendido el comportamiento normal del sistema, avisará de cualquier acción que no cumpla alguna de las reglas de autorización generadas en el modo de aprendizaje.

7.- Conclusiones

Un sistema SCADA es considerado un sistema de control crítico al monitorizar y controlar el rendimiento y disponibilidad de otras infraestructuras consideradas también críticas (por ejemplo, transporte, sistemas de energía, sistemas de administración y tratamiento de agua o sistemas de comunicación).Una interrupción en alguno de sus componentes (hardware o software) debido a un fallo (técnico o humano) o un ataque (físico o lógico), podría suponer un efecto en cascada o un efecto en escalada entre infraestructuras y expandirse consecuentemente hacia demás sectores, afectando a una región, nación o naciones. Estos efectos se deben al tipo de interdependencias (directas o indirectas) entre infraestructuras [1].

Es necesario resolver y mitigar muchos de los problemas identificados en estos tipos de sistemas de control, y prever mecanismos, políticas, estándares y procedimientos de

seguridad para proteger al sistema desde su nivel físico (instalaciones, redes de comunicación y recursos) hasta su nivel lógico (software y canales de comunicación). Actualmente, existen varios documentos técnicos y artículos que describen inconvenientes y algunas soluciones. No obstante, y debido a la criticidad de estos sistemas, es necesario mantener siempre una visualización actualizada de nuevos problemas de seguridad y recomendaciones técnicas.

Por lo tanto, se ha descrito e identificado en este artículo diversos procedimientos de gestión de la seguridad en los IHM, en las redes de comunicación SCADA y control de acceso, identificando nuevas e importantes necesidades, como son: la definición de estándares y políticas de seguridad, especificación de roles y responsabilidades, y diseño e implementación arquitecturas de red segura. Sin embargo, es necesario tener en cuenta otros factores cruciales en estos sistemas críticos, como son la gestión de riesgos (entre ellas destacar RiskMAP destinada a proveer soporte en la toma de decisiones **[**40]), gestión de incidencias para realizar futuros análisis e investigaciones forenses, gestión de documentos, definición de métricas y metodologías de evaluación, proliferación periódica de programas educativos, mantenimiento y auditoría.

8.- Agradecimientos

Este trabajo está bajo el proyecto de investigación CRISIS (TIN2006-09242) y ARES (CSP2007-00004) ambos financiados por el Ministerio de Educación y Ciencia (MEC)

Referencias

[1] **James P. Peerenboom, Ronald E. Fisher**, *Analyzing Cross-Sector Interdependencies*, 40th Annual Hawaii International Conference on System Sciences (HICSS '07), IEEE Computer Society, pp. 112-119, 2007.

[2] **V. Igure, S. Laughter, R. Williams**, *Security issues in SCADA networks*, Computers & Security 25, v 25, pp 498-506, num 7, 2006.

[3] **R. Chandia, J. Gonzalez, T. Kilpatrick, M. Papa, S. Shenoi**, *Security Strategies for SCADA Networks*, IFIP International Federation for Information Processing, Critical Infrastructure Protection, Springer Boston, v 253, pp 117-131, 2007.

[4] **M. Hentea**, *Improving Security for SCADA Control System*, Interdisciplinary Journal of Information, Knowledge, and Management, v 3, pp 73-86, 2008.

[5] **Modbus-IDA** the architecture for distributed automation, http://www.modbus.org/, 2005.

[7] **IEC 60870-6**, International Electrotechnical Commission, [8] **ODVA**, Open DeviceNet Vendors Association, http://www.odva.org/, 2008.

[9] **A. Cárdenas, S. Amin, S. Sastry**, *Research Challenges for the Security of Control Systems*, 3rd USENIX Workshop on Hot Topics in Security (HotSec'08), San Jose, USA, 2008,

[10] **CERT**, Carnegie Mellon Software Engineering Institute, CERT/CC Statistics 1988-2008, http://www.cert.org/stats/vulnerability_remediation.html, 2008.

[11] **BCIT**, British Columbia Institute of Technology, http://www.bcit.ca/, 2008.

[12] **E. Byres, J. Lowe**, *The myths and facts behind cyber security risks for industrial control systems*, 'VDE Congress, VDE Association For Electrical, Electronic Information Technologies, British Columbia Institute of Technology and PA Consulting Group, 2004.

[13] **DEADBOLT**, Institute for Information Infrastructure Protectio (I3P), http://www.thei3p.org/docs/publications/factsheet-Deadbolt-2-24-08.pdf, 2008.

[14] **NIST Special Publication 800-53**. *Recommended Security Controls for Federal Information Systems*, 2007.

[15] **ISO/IEC 17799:2005**. *Code of Practice for Information Security Management*, 2005.

[16] **ISACA**, *Control Objectives for Information and related Technology, rev 4.1*, 2007.

[17] **NIST Special Publication 800-82**. *DRAFT - Guide to Industrial Control Systems (ICS) Security*, 2007.

[18] **D. Kilman, J. Stamp**. *Framework for SCADA Security Policy*. Sandia National Laboratories report SAND2005-1002C. 2005.

[19] **U.S. Department of Energy**, *21 Steps to Improve Cyber Security of SCADA Networks*, white paper, 2005.

[20] **SecSS**, Institute for Information Infrastructure Protection (I3P), http://www.thei3p.org/docs/publications/factsheet-SecSS-2-21-08.pdf, 2008.

[21] **R. Roman, C. Alcaraz, J. Lopez**, *The role of Wireless Sensor Networks in the area of Critical Information Infrastructure Protectio*n, Information Security Technical Report, Elsevier. Vol 12, no 1, pp 24-31, 2007.

[22] **ISA100**, Wireless Systems for Automation, http://www.isa.org/MSTemplate.cfm?MicrositeID=1134&CommitteeID=6891, Industrial Automation and Control system (ISA), 2007.

[23] **WirelessHART™ technology**, , HartComm Company, [24] **NISCC**, National Infrastructure Security Co-ordination Centre, *NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks*, British Columbia Institute of Technology (BCIT), 2005.

[25] **Modbus Software**, Linux Firewall for Modbus/TCP protocol, http://sourceforge.net/projects/modbusfw, 2008.

[26] **Vattenfall**, http://www.vattenfall.se/www/vf_se/vf_se/518304omxva/525894stude/525924exame/564400exemp/833879firew/index.jsp, 2007.

[27] **IEC 60870-5**, International Electrotechnical Commission, [28] **EMERALD**, Event Monitoring Enabling Responses to Anomalous Live Disturbances, SRI International, http://www.sdl.sri.com/projects/emerald/, 2007.

[29] **IDS Signatures**, Digital Bond, http://www.digitalbond.com/index.php/research/ids-signatures/, 2007.

[30] **Nessus 3 SCADA**, Tenable Network Security, http://blog.tenablesecurity.com/2006/12/nessus_3_scada_.html, 2006.

[31] **D. Nicol, B. Sanders, M. Seri**, *Access Control Policies and their Impact on Survivability*, Process Control Systems Workshop, The 4th Annual I3P PCS Security, 2008.

[32] **P. Tsang, S. Smith**, *YASIR: A low-latency high integrity security retrofit for legacy SCADA systems*, 23rd International Information Security Conference (IFIC SEC), 2008.

[33] **IEC-62351**, International Electrotechnical Commission, , [34] **AGA-12 Part 1**, *Cryptographic Protection of SCADA Communications Part1: Background, Policies and Test Plan*, 2006.

[35] **AGA-12 Part 2**, M. Hadley, K. Huston, *Performance Test Plan, Pacific Northwest National Laboratories*, 2006.

[36] **R. Lambert**, *ECC and SCADA Key Management*, SCADA Security Scientific Symposium Conference, Digital Bonded, 2007.

[37] **L. Cambacédes and P. Sitbon**, *Cryptographic Key Management for SCADA Systems -Issues and Perspectives*, pp 156-161, IEEE Computer Society, Information Security and Assurance (ISA) 2008.

[38] **D. Morrill**, *Everybody Panic Metasploit does SCADA Hacking*, Information Technology Professional IT Community, http://it.toolbox.com/blogs/managing-infosec/everybody-panic-metasploit-does-scada-hacking-27104, 2008.

[39] **K. Finisterre**, *The Five Ws of Citect ODBC Vulnerability CVE-2008-2639*, http://www.milw0rm.com/papers/221, 2008.

[40] **RiskMAP**, Institute for Information Infrastructure Protection (I3P), http://www.thei3p.org/docs/publications/factsheet-RiskMap-2-22-08.pdf, 2008.

Biografías

Cristina Alcaraz es estudiante de doctorado y recibió su título como Ingeniera en Informática en 2006 por la Universidad de Málaga. Sus líneas de investigación principales son la protección de las Infraestructuras Críticas de Información y la seguridad de sistemas de control.

Gerardo Fernández es estudiante de doctorado y recibió su título como Ingeniero Informático en 2002 por la Universidad de Málaga. Sus principales líneas de investigación son detección y prevención de intrusiones, seguridad de redes y gestión de vulnerabilidades.

Rodrigo Román recibió su título como Ingeniero Informático el año 2004, y el de Doctor en Informática en 2008, ambos en la Universidad de Málaga. Su principal línea de investigación es la provisión de seguridad en las Redes de Sensores Inalámbricas, así como también la seguridad de entornos ubicuos e Infraestructuras Críticas de Información.

Angel Balastegui recibió el título de Ingeniero Técnico en Informática de Sistemas por la Universidad de Málaga en 2008. Desde 2006 colabora como becario en diversos proyectos de Seguridad en el Dpto. de Lenguajes y Ciencias de la Computación.

Javier López es catedrático del Dpto. de Lenguajes y Ciencias de la Computación, al que se incorporó en 1994. Ha dirigido diferentes proyectos nacionales y europeos en el área de Seguridad de la Información y de las Comunicaciones. Es miembro del consejo editorial de varias publicaciones internacionales.