ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

PRINCIPALES VULNERABILIDADES DE LOS SISTEMAS DE AUTOMATIZACIÓN INDUSTRIAL Y POSIBLES ACCIONES PARA EVITAR CIBERATAQUES

Miguel Ángel Iñigo Ulloa
Departamento de Ingeniería de Sistemas y Automática
ETSI de Bilbao (UPV/EHU), España
minigo@virtualwaregroup.com

Isidro Calvo
Departamento de Ingeniería de Sistemas y Automática
EUI de Vitoria-Gasteiz (UPV/EHU), España
isidro.calvo@ehu.eus

Ismael Etxeberria-Agiriano
Departamento de Lenguajes y Sistemas Informáticos
EUI de Vitoria-Gasteiz (UPV/EHU), España
ismael.etxeberria@ehu.eus

Pablo González-Nalda
Departamento de Lenguajes y Sistemas Informáticos
EUI de Vitoria-Gasteiz (UPV/EHU), España
pablo.gonzalez@ehu.eus

Resumen

Hasta hace unos años, los Sistemas de Control y Automatización Industrial o IACS (Industrial Automation and Control Systems) estaban en gran medida asilados de los sistemas corporativos, lo cual facilitaba su seguridad frente a ciberataques. Sin embargo, la generalización del uso de Internet y las comunicaciones inalámbricas ha cambiado este panorama.
Durante los últimos años se han detectado múltiples evidencias de ciberataques que explotan las vulnerabilidades de los protocolos utilizados en los IACS. Desafortunadamente, estos ataques han ido aumentando de manera significativa en el último lustro, a sabiendas de que sólo termina conociéndose la punta del iceberg.
Este artículo describe en qué consisten algunas de las vulnerabilidades más habituales en los IACS. Así mismo propone una guía básica que busca orientar a los diseñadores y programadores en el nuevo y complejo mundo de la ciberseguridad industrial.

Palabras Clave: Automatización Industrial, Comunicaciones Industriales, Vulnerabilidades, Ciberataques.

1 INTRODUCCIÓN

Los sistemas de control y automatización industrial o *Industrial Automation and Control Systems* (IACS) abarcan varios tipos de sistemas de control entre los que se incluyen los sistemas de supervisión, control y adquisición de datos, *Supervisory Control And Data Acquisition* (SCADA), los sistemas de control distribuidos o *Distributed Control System* (DCS) así como otras configuraciones como los controladores lógicos programables o *Programmable Logic Controllers* (PLCs) o subestaciones de control que están compuestas de dispositivos electrónicos automatizados o *Remote Terminal Units* (RTU).

La introducción de nuevas tecnologías y diferentes tipos de sistemas de comunicación dentro del entorno industrial ha logrado avances significativos en el ámbito del control y la automatización. Por un lado, se han mejorado significativamente las posibilidades de los sistemas SCADA que monitorizan en tiempo real muchas de las infraestructuras críticas en sistemas de energía, transporte, agua, procesos químicos, de gas y de petróleo. Por otro, se ha ampliado el panorama ofreciendo comunicación y conectividad a cualquiera de los dispositivos industriales, especialmente con la introducción de Internet. Además, ya en 2011 la conectividad mediante redes inalámbricas se utilizaba en un 43%

ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

por los operadores y la previsión de crecimiento en su instalación era del 20% en 3 años [1].

Uno de los cambios más significativos del sector industrial en los últimos años ha sido la incorporación de las denominadas tecnologías de la información y de las comunicaciones (TICS). Esta innovación supone un reto para ingenieros e investigadores que han trabajado activamente en la búsqueda y desarrollo de soluciones basadas en Internet y en la mejora del proceso de automatización en términos operacionales [2]. Las mejoras incluyen la capacidad de supervisar y monitorizar procesos con independencia del lugar físico desde el que se accede a los datos, garantizando en todo momento el flujo de información y su rendimiento en tiempo real. Además algunas soluciones basadas el paradigma del *Cloud-Computing* permiten a los investigadores trabajar utilizando interfaces mediante las denominadas arquitecturas orientada a servicios, *Service-Oriented Architecture*. Así, es posible conectar infraestructuras TIC como sensores industriales, contadores inteligentes, Identificadores de Radio-Frecuencia (RFID), teléfonos inteligentes con tecnología inalámbrica dando lugar a un nuevo paradigma identificado como *Internet of Things*, IoT.

Estas nuevas configuraciones han hecho que se cambie la forma de proceder a la hora de crear una red industrial. Tradicionalmente, los sistemas de automatización se encontraban aislados del mundo exterior e Internet de forma que la información que se transmitía desde estas redes a la red de la oficina era mínima [3]. Con la mayor demanda de estos servicios con independencia del punto de acceso y conectividad a sistemas corporativos nos encontramos con que la seguridad de los sistemas de control industrial se ha visto comprometida.

Anteriormente, al verse aislada por completo de los sistemas corporativos y sin acceso a Internet la adopción de hardware y software propietario era suficiente para garantizar un alto nivel de seguridad de los datos. En estos momentos las redes de IACS están amenazadas de manera similar a los sistemas corporativos y es necesario formar redes como las que vemos en la figura 1.

Por otro lado, las medidas de seguridad dentro de los sistemas de control industrial no pueden ser las mismas que en los sistemas de redes corporativas, principalmente por los requisitos de tiempo real y de rendimiento. Por ejemplo, ciertas medidas de seguridad como son las actualizaciones de software requieren paradas y/o reinicios del sistema, algo inviable en sistemas de control industrial.

También encontramos amenazas de origen interno, como sucedió en un incidente tras la infección por el virus Mariposa a través de un dispositivo de conexión USB y que se tardó tres semanas en recuperar la planta industrial [5]. Es por ello que se requiere un plan completo de seguridad que involucre al personal de la empresa.

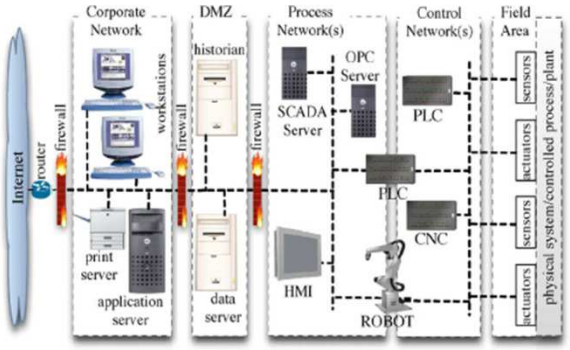

Figura 1: Conexiones típicas de IACS a las redes corporativas e Internet [4]

En los siguientes apartados vamos a analizar las peculiaridades de las comunicaciones de los IACS, identificar sus principales vulnerabilidades en cuanto a ataques cibernéticos y proponer una serie de medidas para garantizar una mayor seguridad en el funcionamiento de dichos sistemas. El artículo acabará con unas conclusiones finales.

2 COMUNICACIONES INDUSTRIALES

2.1 CARACTERISTICAS

Los diferentes componentes que forman un IACS y los que componen la pirámide de automatización (figura 2), cuya implantación se realizó a partir de los años 90 con la aparición de redes basadas en IP, en las redes de área local e Internet [6] o la norma ISA-95 [7], tienen requisitos diferentes en cuanto a funcionamiento y rendimiento de cada nivel, tanto para los sistemas propiamente como para los protocolos de comunicaciones.

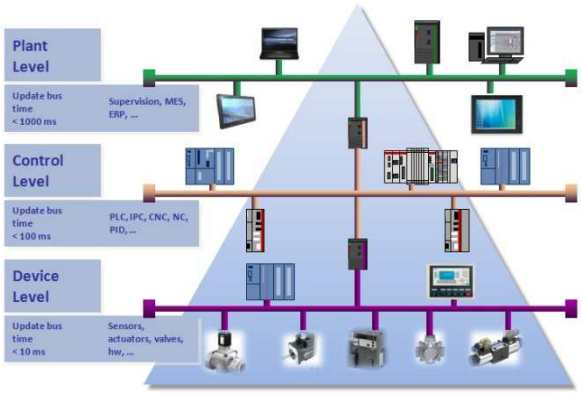

Figura 2: Pirámide de automatización

ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

Los protocolos de comunicaciones utilizan como referencia el modelo básico OSI (*Open System Interconnection*) de 7 niveles, ISO/IEC 7498-1 [8], elaborado por la ISO (*International Standards Organization*). Por el contrario, los protocolos de comunicaciones utilizados en los sistemas industriales son frecuentemente propietarios y diferentes dependiendo del nivel de la pirámide de automatización de uso. A grandes rasgos, estos protocolos se pueden clasificar en la siguiente jerarquía:

- *Nivel de campo*, distribuyendo los datos desde sensores y actuadores hasta controladores y dispositivos de campo.
- *Nivel de control*, distribuyendo la información desde dispositivos de campo hacia controladores y también desde los propios controladores.
- *Nivel de planta*, conectando segmentos de redes a nivel de supervisión, seguimiento y sistemas corporativos.

Las arquitecturas de redes utilizadas en los sistemas industriales tienen más niveles de profundidad que las redes ofimáticas. En estos niveles, fundamentalmente en los niveles inferiores, se usan multitud de protocolos y/o medios físicos que aun siendo similares o incluso idénticos a los utilizados en las redes ofimáticas, requieren pasarelas para facilitar la comunicación con las capas superiores. Esta situación es justo la inversa a la habitual en los sistemas puramente de gestión, donde los protocolos y medios físicos suelen estar más uniformizados.

La mayoría de los protocolos industriales tienen como requisito fundamental cumplir con los requisitos de tiempo real. Así tenemos requisitos de tiempo real:

- *Blandos*, con tiempo de ciclo escalable, utilizado en el nivel de planta y automatización de procesos cuando no hay consecuencias severas si los plazos no se cumplen
- *Severos/duros*, con tiempos de ciclo entre 1 y 10 ms [9] utilizado para el control de bucle cerrado de tiempo crítico
- *Isócrona*, con tiempos de ciclo de 250µs a 1 ms, con fuertes restricciones a la fluctuación (normalmente menos de 1µs), que se utilizan para aplicaciones de control de movimiento

Dichos requisitos de tiempo real dependen del rendimiento del protocolo de comunicación, que a su vez dependen de cuatro parámetros:

- La *latencia*: tiempo que tarda un paquete en atravesar una red
- El *jitter*: variabilidad de la latencia en el tiempo
- El *ancho de banda*
- El *throughput* volumen de datos que pueden fluir a través de una red.

Para tener un buen funcionamiento de tiempo real en una red de sistemas de control industrial se necesita fundamentalmente que:

- Latencia sea baja
- *Jitter* sea constante y bajo.

Sin embargo, es importante tener en cuenta que las posibles soluciones introducidas para mejorar las necesidades de seguridad de los IACS pueden afectar de forma importante al rendimiento de estos parámetros.

3 VULNERABILIDADES DE LOS IACS

Según un informe generado para sistemas de control industrial por el ICS-CERT (*Industrial Control Systems Cyber Emergency Response Team*), el número de incidentes registrados en 2012 se ha multiplicado por cinco desde el 2010 [10] como podemos ver en la figura 3. Uno de los casos más sonados es el gusano *Stuxnet* descubierto en 2010, que operó durante tres años sin ser detectado induciendo daño físico en infraestructuras industriales [11]. En automóviles modernos se ha detectado la posibilidad de ataques cibernéticos pudiendo algunos de ellos llevar a consecuencias físicas [12]. En otro estudio realizado sobre 291 compañías del sector energético en USA el 76% de ellas sufrió uno o más incidentes de seguridad en 2010 [13]. Éstos y otros incidentes han hecho que los gobiernos, las comunidades e investigadores comiencen a prestar especial atención a la seguridad en los sistemas de control industrial.

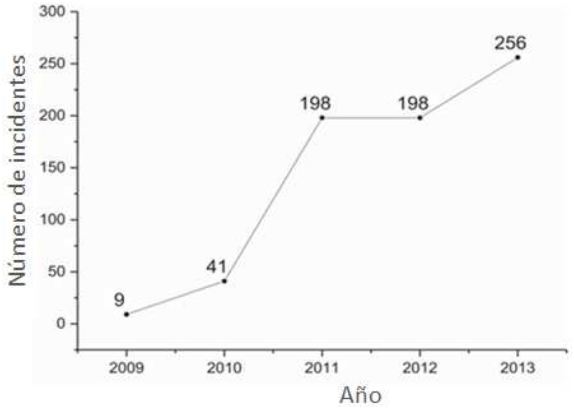

Figura 3: Evolución del número de incidentes [14]

Es importante reseñar que cuando se habla de ataques, nos referimos principalmente a ataques cibernéticos contra equipos industriales englobados dentro del término inglés *Security* y no del *Safety* [15], aunque evidentemente, los fallos de *Security*

ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

pueden producir también fallos de *Safety*. En muchos casos dichos ciberataques aprovechan las vulnerabilidades que ofrecen los Sistemas de Control Industrial y se pueden clasificar en los siguientes tipos según [16] y [17]:

- Políticas y procedimientos
- Plataforma
- Red.

3.1 VULNERABILIDADES DE POLÍTICAS Y PROCEDIMIENTOS

Las vulnerabilidades relacionadas con las políticas y procedimientos para los sistemas de control industrial están relacionadas con:

- Pobre o inadecuada política de seguridad para los IACS sin procedimientos específicos documentados
- Inexistente definición formal de un programa de sensibilización y formación sobre seguridad en los IACS; arquitectura y diseño de seguridad inadecuada
- Directrices de seguridad a implementar en los IACS deficientes o inadecuadas
- Pocas o inexistentes auditorias para los IACS
- Carencia de un plan específico ante desastres
- Brecha relacionada con la gestión del cambio de configuración en IACS específicos.

3.2 VULNERABILIDADES DE PLATAFORMA

En cuanto a las vulnerabilidades de plataforma se deben a la propia plataforma del hardware que la compone, del software y de la protección contra software malicioso o malware. Las más destacadas están relacionadas con:

- Desactualización de equipos y su software, en muchos casos con más de 15 años de vida [3]
- Configuraciones por defecto y/o nulas y/o carencia de copias de seguridad de las configuraciones críticas
- Pérdida de configuraciones por entornos no adecuados y/o saltos de voltaje o pérdida de energía
- Accesos remotos mal configurados o inadecuados
- Contraseñas mal definidas o nulas
- Inadecuados controles de autenticación a equipos y software
- Software mal diseñado ante vulnerabilidades de desbordamiento de buffer [18] o de denegación de servicio (DoS, *Denial of Service*) [19]
- Medidas y/o software inadecuadas o inexistentes sobre el software malicioso
- Uso de servicios innecesarios en funcionamiento.

3.3 APLICACIÓN Y CONFIGURACIÓN DE FIREWALLS

Por último, las vulnerabilidades de red pueden ser de la configuración de la red, del hardware, del perímetro, de la monitorización y autenticación de las comunicaciones y de las conexiones inalámbricas. Todas ellas están relacionadas con:

- Arquitectura de red inadecuada con medidas de seguridad inexistentes o inadecuadas
- Control y configuración del flujo de datos inadecuado
- Configuraciones no almacenadas y/o sin copias de seguridad
- Contraseñas no cifradas y/o con valores por defecto y/o sin cambios en mucho tiempo
- Puertos físicos no asegurados
- Replicaciones inexistentes en redes críticas
- Perímetro de seguridad inexistente
- Cortafuegos inexistentes o mal configurados,
- Configuraciones de control de la red para redes no destinadas a sistemas de control industrial,
- Monitorización inexistente
- Uso de protocolos estándar como telnet o FTP con comunicaciones no cifradas
- Autenticación de los protocolos inexistente en cualquier nivel
- Comprobaciones de integridad inexistentes
- Autenticación entre el cliente inalámbrico y el punto de acceso inadecuada
- Protección de los datos en las conexiones inalámbricas inadecuada.

Las vulnerabilidades más comunes que presentan los protocolos de comunicación, tanto cableados como para comunicaciones inalámbricas son:

- Falta de autenticación de los mensajes
- Falta de cifrado de los mensajes
- Ataques de intermediario, o *Man in The Middle* (MitM)
- Ataques de denegación de servicio (DoS, *Denial of Service*)
- Desbordamiento de búfer o *Buffer*

El ataque de denegación de servicio o DoS se produce cuando un evento malicioso amenaza la disponibilidad de un recurso. Es una categoría de ataque muy amplia por lo que puede incluir desde la perdida de las comunicaciones con el dispositivo hasta inhibir o chocar servicios específicos dentro del propio dispositivo (como almacenamiento o procesamiento de E/S). Los ataques DoS en sistemas corporativos no tienen consecuencias negativas

ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

significativas sin embargo un DoS bien dirigida puede desconectar un sistema y provocar un apagado.

Un búfer es una memoria continua asignada donde se almacenan los datos de proceso. Un desbordamiento de búfer se produce cuando los datos escritos en un búfer debido a la insuficiencia de espacio corrompen los valores de direcciones adyacentes al búfer asignado. Esto permite al sobrescribir los datos que controlan la ruta lógica de programación para secuestrar el programa y ejecutar el programa atacante.

Los ataques de intermediario o MitM son una de las amenazas más populares y desafiantes en los sistemas de computación. Hay gran cantidad de trabajos de investigación dedicados a la detección y al análisis de las diferentes formas de estos ataques [20, 21, 22]. En un ataque MitM un intruso es capaz de leer y escribir mensajes comunicados entre dos partes sin que ninguna de las partes de sea consciente de ello. Este modo de ataque ha evolucionado con los nuevos avances tecnológicos. A modo de ejemplo, en 2004 [23], el servicio CitiBusiness de Citibank fue víctima de un ataque de *phishing* 1.0 (una forma de ataques MitM apuntado para usuarios Web) en la que una página web falsa construida para parecerse a la página del servicio original se utilizó para engañar a los usuarios haciéndoles creer que estaban comunicando con el servicio auténtico, comprometiendo los detalles de su cuenta.

4 ORIENTACIONES DE SEGURIDAD A TENER EN CUENTA

En este apartado se introducen una serie de orientaciones de seguridad que pretenden servir de guía para indicar a los diseñadores qué aspectos se deben de tener en cuenta en el diseño de los sistemas de automatización. Es importante señalar que es imposible conseguir un sistema totalmente seguro frente a ciberataques y, de hecho, en la opinión de los autores, la primera medida de seguridad parte del hecho de ser plenamente consciente de esta premisa.

Existen diversas formas de proteger los sistemas de control industrial frente a las amenazas provenientes del exterior, p.e. a través de la conexión con Internet, así como de las vulnerabilidades anteriormente descritas:

- Controlar los servicios en ejecución y/o puertos abiertos que no se utilizan
- Cifrar las comunicaciones
- Implementar servicios de seguridad en TCP/IP
- Gestionar las claves adecuadamente (p.e. con algún sistema de gestión de claves)
- Usar adecuadamente los cortafuegos (o firewalls)
- Usar sistemas de prevención y/o detección de intrusiones (IDS)
- Usar paquetes antivirus/antimalware
- Implementar redes privadas virtuales (VPN) basadas en IPSec [24] así como otros mecanismos descritos en [25].

En el caso del diseño de una arquitectura de red que afecte a IACS es recomendable separarla de la red corporativa. La naturaleza de estas dos redes es diferente: el acceso a Internet, FTP, email y acceso remoto está permitido en redes corporativas pero no en redes IACS. Si el tráfico de red de un sistema de control industrial se realiza en la red corporativa, podría ser interceptada o ser objeto de un ataque de DoS. En el caso de que fuera necesaria la conexión de las dos redes se hace indispensable la implantación de:

- Un cortafuegos
- Una Red Desmilitarizada (DMZ) [26].

La configuración adecuada de los cortafuegos (o firewalls) es fundamental ya que permite:

- Restringir considerablemente el acceso no deseado hacia y desde los ordenadores y los controladores de host del sistema de control, mejorando así la seguridad
- Mejorar potencialmente la capacidad de respuesta de una red de control mediante la eliminación del tráfico no esencial de la red.

Por otro lado existen cuestiones que hay que tener en cuenta al desplegar cortafuegos en ambientes de IACS. En particular, la adición de retardo en las comunicaciones o la complejidad de establecer una configuración adecuada para aplicaciones industriales.

A pesar de que no sirva siempre la misma estrategia para evitar cualquier amenaza y resolver las vulnerabilidades, una estrategia global y en profundidad se basa en las siguientes políticas, que se amplían en las siguientes subsecciones [16]:

- El uso de cortafuegos
- La creación de zonas desmilitarizadas
- La implantación de medidas de detención de intrusos con respuesta ante incidentes
- Una política de seguridad y programas de formación
- Un conocimiento profundo de los ataques que se producen en los sistemas de control industrial los que incluyen.

ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

4.1 APLICACIÓN Y CONFIGURACIÓN DE CORTAFUEGOS

Un cortafuegos bien configurado permite restringir considerablemente el acceso no deseado hacia y desde los ordenadores y los controladores de host del sistema de control, mejorando la seguridad así como potencialmente mejorando la capacidad de respuesta de una red de control mediante la eliminación del tráfico no esencial de la red.

Su configuración permite crear reglas para algunos servicios específicos tales como DNS, HTTP, FTP o TFTP, telnet, SMTP, SNMP, DCOM, los sistemas SCADA y Protocolos industriales. Para los IACS hay que considerar una serie de cuestiones relacionadas con la configuración de los cortafuegos como son: el acceso remoto, el tráfico *Multicast*, puntos únicos de fallo, redundancia y tolerancia a fallos y prevención de ataques MitM.

Una configuración muy básica que podría funcionar en un gran número de casos, a pesar de la penalización de rendimiento del cortafuegos, incluiría las siguientes acciones:

- Denegar todas las comunicaciones excepto las marcadas como conocidas y aceptadas
- Especificar las direcciones IP de origen y de Destino
- Utilizar inspecciones de datos para controlar las conexiones activas y así decidir qué paquetes tienen autorización
- Usar inspección profunda de paquetes para controlar el contenido del tráfico en las comunicaciones y no solo en las cabeceras
- Forzar a no utilizar los mismos protocolos de comunicaciones entre la red corporativa y la DMZ y la DMZ y la red de sistemas de control industrial.

4.2 FILTRADO Y SEGMENTACIÓN MEDIANTE DMZ

Una DMZ [26] o red desmilitarizada es una zona aislada que corresponde a una red entre la red privada de la empresa y el exterior. La DMZ previene a los usuarios externos de un acceso directo a dicha zona dotándole de una seguridad, control y filtrado mayor. Existen diferentes configuraciones y arquitecturas de redes para los sistemas de control.

4.3 CONTROL DE ACCESOS Y COMUNICACIONES SEGURAS

En el control de accesos hay que identificar cómo se accede y desde dónde se accede siguiendo las recomendaciones de identificación unívoca, autorización basada en roles y principio de mínimo privilegio con conexiones limitadas, filtración por puertos, aplicaciones y usuarios y mediante comunicaciones cifradas. Conviene utilizar VPNs para asegurar el tráfico entre extremos y así evitar que la información pueda ser capturada.

Hay que tener precaución con los mecanismos de cifrado utilizados para que no generen una DoS de los dispositivos implicados. Además, se debe tener en cuenta los efectos que puede introducir en la latencia y en el *jitter* para cumplir con los requisitos de tiempo real de las aplicaciones.

4.4 MONITORIZACIÓN EN REDES DE SISTEMAS DE CONTROL INDUSTRIAL

En los sistemas de control y automatización se recomienda monitorizar y ajustar cada uno de los sensores, enviar alertas, revisar los eventos generados y configurar correctamente los equipos.

Los sistemas IDS permiten monitorizar las redes y detectar su mal uso o anomalías en funcionamiento. En el primer caso se compara las conexiones de red con las grandes bases de datos de firmas de ataques conocidos. En el segundo caso define una línea base y compara su funcionamiento con segmentos de otras redes para detectar anomalías.

En cualquier caso hay que definir qué se va a monitorizar, analizar los logs, comparar y tomar decisiones.

4.5 PREVENCIÓN CONTRA EL MALWARE

Se conoce como Malware cualquier tipo de software malicioso o molesto que puede instalarse en los sistemas informáticos para llevar a cabo acciones sin conocimiento del usuario. Existen diferentes tipos de malware siendo los virus los más conocidos.

Los paquetes antivirus analizan archivos en dispositivos de almacenamiento contra un inventario de archivos de firmas de malware conocidos. El software antivirus se puede implementar en estaciones de trabajo, servidores, firewalls y dispositivos de mano. Su uso en IACS puede requerir la adopción de prácticas especiales, incluyendo controles de compatibilidad, cambios de gestión y las métricas de rendimiento de impacto.

5 CONCLUSIONES

Los sistemas de control industrial se encuentran frecuentemente amenazados por ataques cibernéticos debido a la nula o pobres medidas de seguridad implementadas por su aislamiento a sistemas externos a ellos. Las nuevas arquitecturas de redes necesarias por la conectividad entre las redes

ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

corporativas y las industriales con la eclosión a Internet han puesto en riesgo su respuesta, la productividad y continuidad de dichos entornos como venían funcionando hasta este momento.

En el presente artículo se ha analizado cómo muchas de las vulnerabilidades más comunes se deben a falta de autenticación y autenticación, falta de cifrado de los mensajes, ataques *Man in the Middle*, ataques *Denial of Service*, ataques *Zero-day* y desbordamiento de Buffer.

Es importante señalar que es imposible conseguir un sistema totalmente seguro frente a ciberataques y, de hecho, en la opinión de los autores, la primera medida de seguridad parte del hecho de ser plenamente consciente de esta premisa. Sin embargo, los autores introducen un conjunto de orientaciones de seguridad que pretenden servir de guía para indicar a los diseñadores qué aspectos se deben de tener en cuenta en el diseño de los sistemas de automatización. También es importante asumir que muchas de las medidas de seguridad requieren la introducción de algoritmos sofisticados, por ejemplo de encriptación de datos, que pueden afectar al rendimiento global de los sistemas.

Por último, se ha detectado que es necesaria la implementación de estrategias globales y en profundidad mediante políticas que afecten tanto al nivel de red y de plataforma que proporcionen ciertas medidas de seguridad.

Agradecimientos

Este trabajo ha sido subvencionado por el Gobierno Vasco/Eusko Jaurlaritza a través del proyecto CPS4PSS ETORTEK14/10 y por la Universidad del País Vasco/Euskal Herriko Unibertsitatea (UPV/EHU) por medio del proyecto EHU13/42 y la UFI11/28.

Referencias

[1] Boyes, W., (2011) “All quiet on the wireless front”, Control, 9 de agosto de 2011, http://www.controlglobal.com/articles/2011/all-quite-on-the-wireless-front/

[2] Jain, M., Jain, A., Srinivas, M., (2008) “A web based expert system shell for fault diagnosis and control of power system equipment”, Proceedings of International Conference on Condition Monitoring and Diagnosis (CMD-08), 2008, pp. 1310–1313.

[3] Fischer, K., Gesner, J., (2012) “Security Architecture Elements for IoT enabled Automation Networks”, 17th IEEE Intl. Conf. Emerging Technologies and Factory Automation (ETFA).

[4] Cheminod, Manuel, Luca Durante, and Adriano Valenzano. "Review of security issues in industrial networks." Industrial Informatics, IEEE Transactions on 9.1 (2013): 277-293.

[5] Sinha, P., Boukhtouta, A, Belarde, V.H., Debbabi, M., (2010) “Insights from the Analysis of the Mariposa Botnet”, 5th IEEE Int. Conf. Risks and Security of Internet and Systems (CRiSIS).

[6] Schwaiger, C., Treytl, A. (2003) “Smart card based security for fieldbus systems”, 5th IEEE Intl. Conf. Emerging Technologies and Factory Automation (ETFA).

[7] Scholten, B. (2007) “The Road to Integration: A Guide to Applying the ISA-95 Standard in Manufacturing”, International Society of Automation (ISA).

[8] Standardization, I. O. F. "ISO/IEC 7498-1: 1994 information technology–open systems interconnection–basic reference model: The basic model." International Standard ISOIEC 74981 (1996): 59..

[9] Branicky, M.S., Phillips, S.M., Zhang, W. (2000) “Stability of networked control systems: Explicit analysis of delay,” in Proc. American Control Conference (AACC), pp. 2352–2357.

[10] ICS-CERT (2012) “ICS-CERT Monitor Newsletters”, October–December 2012. https://ics-cert.us-cert.gov/monitors

[11] McDonald, G., Murchu, L.O., Doherty, S., Chien, E., (2013) “Stuxnet 0.5: The Missing Link”, Symantec, Mountain View, California.

[12] Checkoway, S., McCoy, D., et al. (2011) “Comprehensive experimental analyses of automotive attack surfaces”, Proc. 20th USENIX Conf. on Security.

[13] Ponemon Institute (2011) “State of IT Security. Study of Utilities & Energy Companies”.

[14] Yang, Wen, and Qianchuan Zhao. "Cyber security issues of critical components for industrial control system." Guidance, Navigation and Control Conference (CGNCC), 2014 IEEE Chinese. IEEE, 2014.

[15] Kriaa, S., et al. (2015) “A survey of approaches combining safety and security for industrial

ISBN 978-84-15914-12-9 © 2015 Comité Español de Automática de la IFAC (CEA-IFAC)

control systems", Reliability Engineering & System Safety, 139, pp. 156-178.

[16] Stouffer, Keith, Joe Falco, and Karen Scarfone. "Guide to industrial control systems (ICS) security." NIST special publication (2011): 800-82.

[17] Eric D. Knapp and Joel Thomas Langill, Chapter 8 - Risk and Vulnerability Assessments, In Industrial Network Security (Second Edition), edited by Eric D. KnappJoel Thomas Langill, Syngress, Boston, 2015, Pages 209-260.

[18] Feifei, L., (2012) "The principle and prevention of windows buffer overflow", 7th Intl. Conf. Computer Science & Education (ICCSE).

[19] Liu, W., (2009) "Research on DoS attack and detection programming", 3rd IEEE Intl. Symp. Intelligent Information Technology Application (IITA), pp. 207-210.

[20] Asokan, N., Niemi, V.,Nyberg, K. (2003) "Man-in-the-Middle in Tunnelled Authentication Protocols", Security Protocols Workshop, volume 3364 of LNCS, pages 28-41. Springer.

[21] Kügler, D., (2003) ""Man in the Middle" Attacks on Bluetooth", Financial Cryptography, volume 2742 of LNCS, pages 149-161. Springer.

[22] Meyer U., Wetzel, S. (2004) "A man-in-the-middle attack on UMTS", Proc. 3rd ACM Workshop on Wireless Security (WiSe), pp. 90-97.

[23] Aziz, B., Hamilton G., (2009) "Detecting man-in-the-middle attacks by precise timing", 3rd IEEE Intl. Conf. Emerging Security Information (SECURWARE).

[24] Heng, Y., Wang, H. (2007) "Building an application-aware IPsec policy system", IEEE/ACM Trans on Networking, 15:6 pp. 1502-1513.

[25] Hadziosmanovic, D., Bolzoni, D., Hartel, P. (2012) "A log mining approach for process monitoring in SCADA", Intl. Journal of Information Security (IJIS) 11:4 pp. 231–251.

[26] Flynn, H. (2006) "Designing and building enterprise DMZs", Syngress.