Sistema visual de monitorización de seguridad de flujos de red industriales

Mikel Iturbe, Iñaki Garitano, Urko Zurutuza, Roberto Uribeetxeberria

Dpto. de Electrónica e Informática
Escuela Politécnica Superior
Mondragon Unibertsitatea
Email: {miturbe, igaritano, uzurutuza, ruribeetxeberria}@mondragon.edu

Resumen— **Los sistemas de control industrial son el conjunto de elementos especializados que monitorizan y controlan procesos físicos. Estos sistemas están generalmente interconectados en entornos conocidos como redes industriales. Las particularidades de este tipo de redes desaconseja el uso de herramientas de seguridad utilizadas en redes tradicionales de computadoras, mientras que a la vez permiten la utilización de estrategias de seguridad no extrapolables a redes de computadoras. El uso de listas blancas ha sido probado como un enfoque válido para asegurar redes industriales. En este artículo presentamos un sistema visual de monitorización y detección de anomalías de flujo que utiliza listas blancas y diagramas de cuerdas para mostrar el estado de la red. Por último se utilizan datos de una red industrial real para probar la efectividad del sistema.**

I. Introducción

Los Sistemas de Control Industrial (SCIs) son el conjunto de elementos especializados que monitorizan y controlan procesos físicos [1]. Como tal, son los responsables de controlar y automatizar una gran variedad de procesos, tanto en diferentes sectores industriales o en Infraestructuras Críticas (ICs) [2], generalmente en entornos conectados conocidos como redes industriales. El Consejo de la Unión Europea [3] define los ICs como "el elemento, sistema o parte de este (...) que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;". Ejemplos de infraestructuras críticas incluyen la generación y transporte de energía, el suministro de agua, sistemas de transporte o plantas de fabricación críticas.

Tradicionalmente, las redes industriales han formado entornos aislados, con protocolos de red, software y hardware propietarios. Sin embargo, los SCIs han ido evolucionando hacia la utilización de sistemas de software y red estándares, y hoy en día las redes industriales comparten importantes similitudes con redes de computadoras tradicionales y están cada vez más conectadas a ellas. Esto significa que el aislamiento tradicional en el cual las redes industriales se han basado para su protección ya no es tal; las redes industriales no están tan aisladas. Por ello, la superficie de ataque a estas redes ha aumentado.

Los incidentes de seguridad relacionados con redes industriales han mostrado el gran impacto que puede llegar a tener un ataque exitoso, desde pérdidas económicas, a daños medioambientales o incluso pérdida de vidas humanas [4]. El avance reciente de las Amenazas Persistentes Avanzadas (APTs por sus siglas en inglés) como Stuxnet [5], Night Dragon [6] o Havex [7] que tienen como objetivo las redes industriales, bien para sabotearlas o para el robo de de información, hace aún más necesaria la protección de estos sistemas.

Aunque las redes industriales y las redes de ordenadores tradicionales comparten tecnologías en gran medida, la distinta naturaleza de las redes requiere que las soluciones de seguridad que se aplican en una u otra tengan que ser diseñadas para adecuarse al tipo de red. Las diferencias entre los dos tipos de red y el impacto que ello supone a la hora de diseñar soluciones de seguridad es analizado por Cheminod et al [8].

Cuando se comparan las redes industriales con redes tradicionales de ordenadores, se puede apreciar que la topología de de la red industrial es estática, a la vez que el tráfico de red cuenta con unos patrones de comportamiento muy definidos ya que la mayoría del tráfico de red lo crean procesos automáticos [8], [9].

Teniendo en cuenta estos rasgos de las redes industriales, se puede hacer uso de ellas para diseñar soluciones de seguridad, que aunque válidas para las redes industriales, podrían no ser eficientes en otros tipos de red. Específicamente, la práctica del whitelisting o listas blancas[1] ha sido defendido por la industria como un método efectivo de asegurar redes industriales [2], [10], hecho que fue demostrado por Barbosa et al. [9].

A. Contribución y organización del artículo

En este artículo proponemos un sistema novedoso de monitorización visual de redes industriales a gran escala para monitorizar flujos de red y detectar anomalías relacionadas. Para ello nos valemos de listas blancas y diagramas de cuerdas. Nuestra principal contribución consiste en la creación de listas blancas temporales y la utilización de diagramas de cuerdas para la visualización de flujos de red industriales y sus anomalías. En consecuencia, este artículo pretende cubrir el vacío actual en sistemas de monitorización para la seguridad visuales en redes in-

[1]Es la práctica de registrar una serie de flujos de red permitidos y no permitir ninguna otra conexión o notificar mediante una alerta cuando se produce una conexión no permitida

dustriales.

El resto del artículo está organizado de la siguiente manera: la sección II presenta diferentes detectores de anomalías que utilizan información de flujo, junto con una introducción a los diagramas de cuerdas y su uso en el campo de la seguridad de redes. La sección III analiza la estructura del sistema de monitorización, así como su funcionamiento. La sección IV muestra las pruebas realizadas al sistema con datos de tráfico industrial real. Por último, la sección V extrae unas conclusiones finales e identifica unas posibles vías de trabajo futuro.

II. Trabajos relacionados

A. Detección de anomalías de flujo en redes industriales

Barbosa et al. [9] demostraron que el uso de listas blancas es un método efectivo para detectar anomalías de flujo en redes industriales. Ha habido diferentes sistemas de detección de intrusiones para redes industriales que se han valido de información de flujo para detectar anomalías: Garitano et al. [11] utilizan la información de flujo contenida en forma de reglas de Snort para alertar sobre conexiones anómalas. Hoeve [12] extrae la información de flujo de red y sus patrones, para detectar anomalías que quedan fuera de los patrones en tráfico de control cifrado. SPEAR [13] utiliza la información de la topología de red e información de flujo introducida a mano para detectar anomalías de flujo mediante la creación de reglas para Snort.

Sin embargo, ninguna de las propuestas señaladas presenta los resultados de la detección ni el estado de la red de manera visual.

B. Diagramas de cuerdas

Los diagramas de cuerdas, también conocidos como diagramas Circos, son diagramas circulares que representan las interrelaciones entre diferentes entidades. Aunque originalmente fueron diseñadas para ser utilizadas en genómica [14], el uso de los diagramas de cuerdas se ha extendido a diferentes campos.

Las entidades visualizadas están ordenadas de manera circular. Cada entidad ocupa una longitud de arco diferente en función del peso que tiene en relación al resto de entidades.

Las cuerdas son uniones que conectan las diferentes entidades que forman el círculo. Cada cuerda une generalmente dos entidades diferentes, y la anchura de la cuerda en cada borde indica la naturaleza de la unión. Si uno de los bordes de la cuerda tiene una mayor anchura, la entidad de ese lado tiene una posición más dominante. Por ejemplo, en el caso de que una cuerda represente una relación mercantil entre dos estados, el estado con la cuerda más ancha en su base envía más bienes hacia el estado con la anchura más pequeña que viceversa.

En el campo de la ciberseguridad, los diagramas de cuerdas se han utilizado en diferentes tipos de sistemas de visualización, pero su uso no está tan extendido como otros tipos de diagramas.

Mazel et al. [15] utilizan diagramas de cuerdas para realizar una comparativa visual de diferentes sistemas de detección de anomalías y su rendimiento.

El trabajo de Layton et al. [16] representa las relaciones entre grupos de páginas webs de *phishing* mediante diagramas de cuerdas.

OCEANS [17] utiliza diagramas de cuerdas para representar flujos de redes entre diferentes subredes. Sin embargo, es una solución orientada a redes tradicionales de ordenadores y se limita a mostrar los flujos de red existentes, pero sin mostrar la información de flujos de hosts individuales ni resaltar las anomalías.

De momento, no hay ejemplos de sistema de visualización de flujos orientado a la seguridad para redes industriales, menos aún utilizando diagramas de cuerdas. Sin embargo, se están haciendo varios avances para mejorar la monitorización visual de procesos industriales [18].

III. Descripción del sistema

La figura 1 muestra el flujo de trabajo del sistema de monitorización y visualización presentado.

En primer lugar, dispositivos de red con capacidad de registrar flujos de red envían paquetes con la información de flujo a un recolector de flujos que almacena luego éstos en un servidor de flujos. El envío se puede realizar desde diferentes redes industriales, permitiendo la monitorización central de las redes industriales.

Una vez empezada la recolección de flujos, mediante una consulta al servidor de flujos se crea las políticas de whitelisitng con los primeros flujos recogidos de la red. A esta fase la hemos llamado la fase de aprendizaje. Una vez que las políticas se han creado y se siguen registrando nuevos flujos de red, se realizan consultas adicionales al servidor de flujos para obtener los últimos resultados y luego los compara con las políticas establecidas en las listas blancas para detectar si los flujos nuevos son legítimos o no, etiquetando cada flujo como legítimo o ilegítimo. Esta fase es la fase de detección. Finalmente, una vez los flujos están etiquetados, el sistema crea una serie de diagramas de cuerdas para representar los resultados. Mientras que la fase de aprendizaje ocurre una única vez por red monitorizada, las fases de detección y visualización se repiten periódicamente en el tiempo.

A. Fase de aprendizaje

En esta fase, se crea una lista blanca de flujos a partir de los primeros flujos detectados en una red industrial en un periodo de tiempo determinado. La duración adecuada del periodo de tiempo depende del tipo de proceso que controla la red. En procesos por lotes cortos, la duración necesaria para recoger todos los flujos importantes es menor que en procesos más largos o contínuos, ya que los ciclos de la red serán también más cortos.

La lista blanca es generada en formato CSV, de este modo, un operador humano puede añadir flujos de red que considere oportunos, o borrar los flujos de red registrados que deben ser consideraros anómalos.

En las listas blancas, se guarda la siguiente información por cada flujo: dirección IP origen, dirección IP destino, puerto del servidor, tipo de protocolo IP y el número paquetes de red un intervalo de tiempo dado. No se tiene en

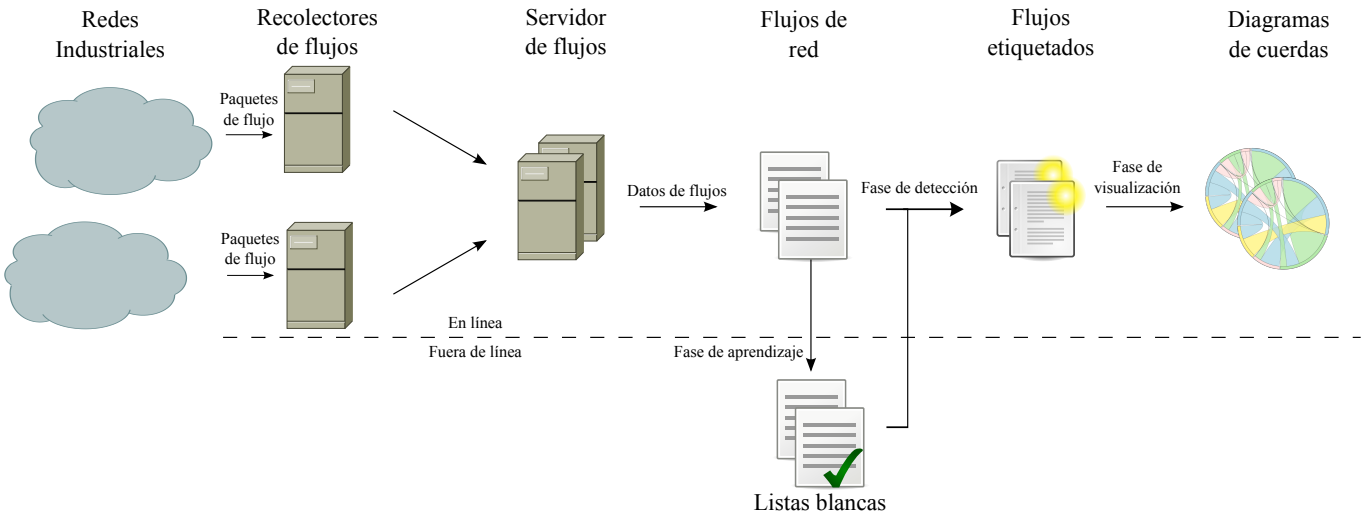


Fig. 1: Vista general del sistema de monitorización de flujos.

cuenta el puerto del cliente, ya que se asigna de manera aleatoria y etiquetar flujos válidos como anómalos por tener un número de puerto cliente distinto daría falsos positivos. Barbosa et al. [9] no tienen en cuenta el número de paquetes para la elaboración de la lista blanca, sin embargo, este sistema sí lo contempla. Consideramos el número de paquetes un atributo importante por dos razones: en primer lugar, para poder utilizar este número como una métrica a de visualización (así ayudaría a mostrar visualmente flujos más y menos activos); y en segundo lugar, puede ayudar a detectar anomalías de flujo relativas al tamaño (ataques de denegación de servicio, o la caída de un dispositivo).

A.1 Listas blancas con datos de flujo temporales

Sin embargo, la utilización del número de paquetes existente en un flujo complica la utilizacón de las listas blancas. El número de paquetes detectado en el flujo es un dato temporal, es decir, dependiente de la duración de la captura (cuanto mayor sea el tiempo monitorizado del flujo, mayor será el número de paquetes que aparecen en él). Por ello, es necesario establecer una validez de un espacio de tiempo a cada lista blanca, en la cual puede ser utilizada. En otras palabras, una lista blanca es solo relevante si el tiempo de captura que se ha utilizado para su elaboración es de la misma duración que los datos de flujo capturados con los que se compara. Por ejemplo, si una lista blanca registra la actividad de una red los primeros diez minutos de una red industrial, es necesario que las capturas de flujos posteriores tengan también la misma duración para poder comparar correctamente el número de paquetes registrado en el flujo.

Hay dos formas diferentes de abordar esta cuestión:

1. Se crea una única lista blanca por red, con los datos registrados de una duración única. Todos los datos de flujos entrantes se recogen, y más tarde, al realizar las consultas, estos datos recogidos se dividen en pedazos donde la duración de la captura de cada pedazo es la misma que la de la lista blanca. El pedazo más reciente se compara con los datos de la lista blanca y se crea un diagrama de red con la información por cada red.
2. Se crean varias listas blancas por cada red, donde cada lista blanca tiene una duración diferente. Todos los datos de flujos entrantes se recogen, y dependiendo de la lista blanca con la que se quiere comparar se dividen en pedazos de duración diferentes. Los últimos pedazos de cada duración se compara con su lista blanca correspondiente. Se crea un diagrama de cuerdas por cada pedazo de duración diferente.

La segunda es una opción más deseable, ya que ofrece más granularidad, dando la oportunidad de monitorizar diferentes ventanas de tiempo y de detectar anomalías que pueden ser clasificadas como falsos negativos cuando se utiliza una única lista blanca. Por ejemplo, si un dispositivo de red está programado para enviar un gran número de paquetes de manera estacional durante periodos cortos, pero debido a un fallo ese envío no cesa, las listas blancas de corta duración permitirán el tráfico, ya que está registrado que el dispositivo envía ese tráfico por periodos cortos. Sin embargo, las listas blancas de mayor duración registraran que a largo plazo no es un tráfico legítimo.

Por ello, proponemos un sistema que utiliza listas blancas con datos de red correspondiente a diferentes periodos de tiempo. Sin embargo, el número óptimo de listas blancas a utilizar, así como la duración de la monitorización de cada lista es un atributo que depende del proceso y debería estudiarse para cada caso. No obstante, es importante recalcar que a mayores tiempos de aprendizaje para construir las listas blancas, mayor es la probabilidad de registrar tráfico malicioso o anómalo en la red y etiquetarlo como legítimo en la lista blanca.

B. Fase de detección

En esta fase, se utilizan las listas blancas creadas en la fase anterior para evaluar los datos de flujo entrantes. Los datos de flujos se obtienen mediante consultas al servidor de flujos. Periódicamente se obtienen los datos de flujos de red correspondientes a los diferentes periodos de tiempo

para los que se haya creado una lista blanca. Después, se comparan los datos de flujo de cada duración con su lista blanca correspondiente.

Por cada flujo detectado, el detector comprueba si los datos del flujo están registrados en la lista blanca. En el caso de las direcciones origen y destino, puerto del servidor y protocolo utilizado, la información de ambos flujos debe ser exacta. En el caso del número de paquetes registrados hay una excepción: los numeros de la lista blanca y del flujo detectado no tienen que ser exactamente iguales, pero tampoco pueden muy diferentes. El detector da la posibilidad de establecer un umbral en forma de porcentaje que indica la tolerancia del detector a la diferencia del número de paquetes registrado. Flujos que difieren del flujo registrado en la lista blanca por un margen mayor que el porcentaje establecido, son etiquetados como anómalos, mientras que los que quedan dentro de los límites del umbral se consideran legítimos.

Si el flujo detectado es considerado válido, el flujo se etiqueta como legítimo y no se lanza ninguna alerta. Sin embargo, si se detecta un flujo que no ha sido registrado en la lista blanca, el detector etiqueta ese flujo como anómalo y lanza una alerta. Además, el sistema también comprueba si los flujos registrados en la lista blanca han sido detectados en la red durante ese periodo de tiempo. Si un flujo registrado en la lista blanca no ha sido detectado, el flujo se añade al grupo de flujos etiquetados como ausente y se lanza una alerta. De esta forma se puede detectar cuando hay problemas de conectividad en la red.

Se han creado las siguientes etiquetas en el detector, basadas en las comparaciones entre las listas blancas y los flujos registrados:

Flujo legítimo El flujo es legítimo según la información contenida en la lista blanca.

Flujo anómalo Dos dispositivos se comunican entre sí, pero según la lista blanca no deberían de hacerlo. Todos los flujos relativos a un dispositivo desconocido se etiquetan como tal.

Puerto incorrecto Un dispositivo trata de conectarse a un puerto diferente del habitual de un dispositivo con el que tiene permitido comunicarse.

Protocolo incorrecto Un dispositivo trata de conectarse a un dispositivo con el que puede comunicarse utilizando un protocolo distinto del habitual.

Flujo ausente Un flujo registrado en la lista blanca no ha sido detectado en el periodo de tiempo correspondiente a la captura.

Tamaño de flujo anómalo El número de paquetes de un flujo registrado en la lista blanca y el flujo detectado varía más que el umbral establecido.

Cada etiqueta se utiliza para dar información acerca de la razón por la que el flujo se considera no legítimo, tanto en la alerta lanzada como en la visualización mostrada.

Una vez que todos los flujos han sido etiquetados, el detector traduce todas las direcciones IP de los dispositivos a nombres de dispositivo para facilitar la comprensión de los datos de flujo al usuario.

Finalmente, después de la traducción de nombres, el sistema tiene un conjunto de flujos completamente etiquetado. Esta información etiquetada se utiliza en la siguiente fase (la de visualización) para construir el diagrama de cuerdas que muestra los flujos de red con sus anomalías detectadas.

C. Fase de visualización

En esta fase, cada uno de los conjuntos etiquetados de flujos de red es mostrado en forma de un diagrama de cuerdas.

En primer lugar, cada uno de los dispositivos activos en la red obtiene una sección de la circunferencia que forma el exterior del diagrama de cuerdas. La longitud de arco es proporcional al porcentaje de paquetes que el host ha enviado en el periodo que ha durado la captura; los dispositivos que envían más paquetes ocupan una longitud de arco mayor. Una vez que los dispositivos han sido colocados en el diagrama, es necesario representar los flujos entre ellos.

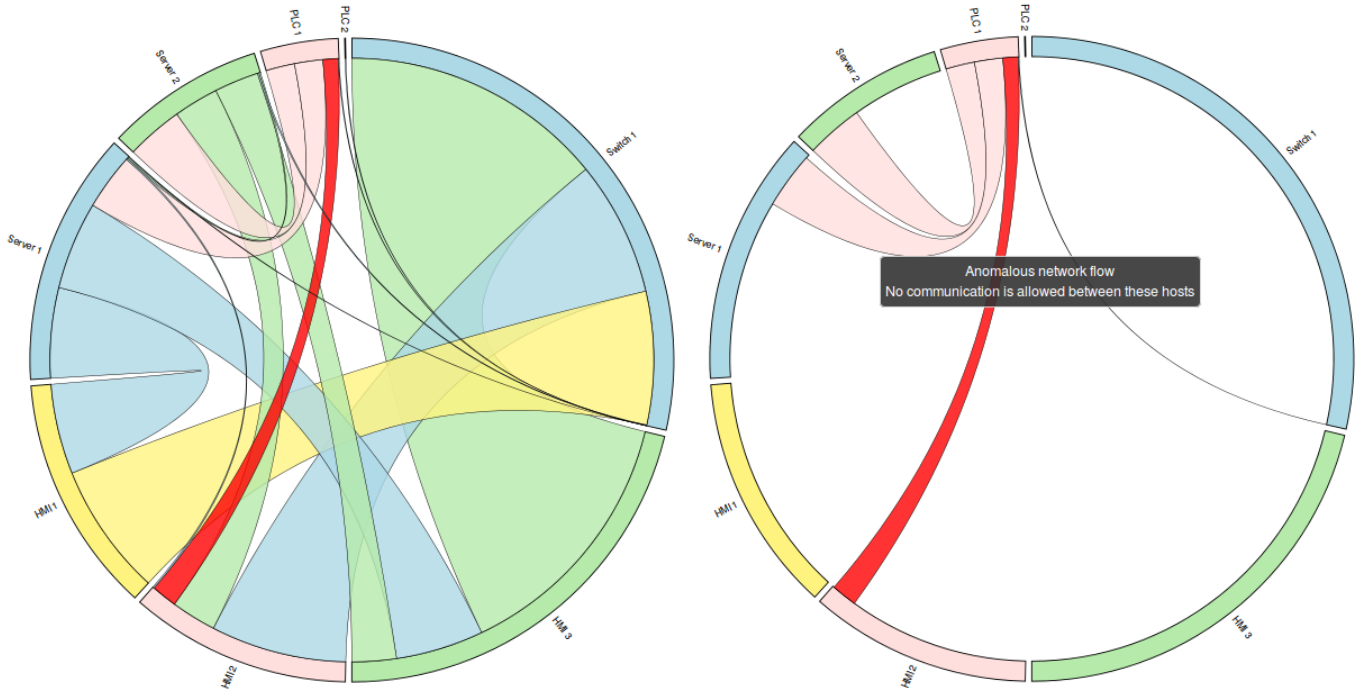
Para ello se utilizan las cuerdas: cada flujo de red bidireccional está representado con una cuerda que une dos dispositivos diferentes. Si dos dispositivos se comunican con diferentes flujos (conexiones a puertos diferentes, uso de protocolos distintos), se sigue visualizando una única cuerda que aglutina los flujos entre los mismos dispositivos.

La anchura en los bordes de la cuerda, viene dado también por el número de paquetes que envía. Por ejemplo, si en un flujo dado el Dispositivo A manda más paquetes que el Dispostivo B, la anchura será mayor en el borde del lado del Dispositivo A. De manera similar, los flujos más activos estarán representados con cuerdas más anchas, ya que los actores más activos tendrán bordes más anchos. El diagrama es interactivo, cuando el usuario pasa el ratón por encima de un flujo, el diagrama muestra información básica acerca del flujo: nombre de los dispositivos implicados, número de paquetes enviados en cada dirección...

La figura 2 muestra un diagrama de cuerdas completo donde todos los flujos detectados en su periodo de tiempo han sido etiquetados como legítimos. Se puede apreciar como la anchura de las cuerdas y sus bordes varía de un flujo a otro dependiendo de la actividad del flujo.

En el caso de flujos de red no legítimos, se rellena de color rojo, como se muestra en la figura 3. Por un lado la figura 3a representa como el color rojo destaca entre el resto de colores de los flujos legítimos. Por otro lado, la figura 3b muestra la interactividad del gráfico: el diagrama filtra los flujos relevantes de un dispositivo y muestra el aviso acerca de la razón por la que el flujo ha sido etiquetado como no legítimo, cuando el usuario selecciona el flujo. Como se ha comentado anteriormente, está información adicional se toma de la etiqueta que ha asignado el detector. En este caso, la lista blanca no permite ningún tráfico entre los dispositivos PLC 1 y HMI 2.

Con la excepción de los flujos con la etiqueta de "Flujo ausente", todos los flujos no legítimos se tiñen de rojo para que destaquen entre el resto de flujos. Sin embargo, debido a la naturaleza diferente de los flujos etiquetados como ausentes, estos flujos son representados teñidos de



(a) Flujo prohibido entre PLC 1 y HMI 2.

(b) Detalle del flujo anómalo

Fig. 3: Representación de un flujo de red anómalo.

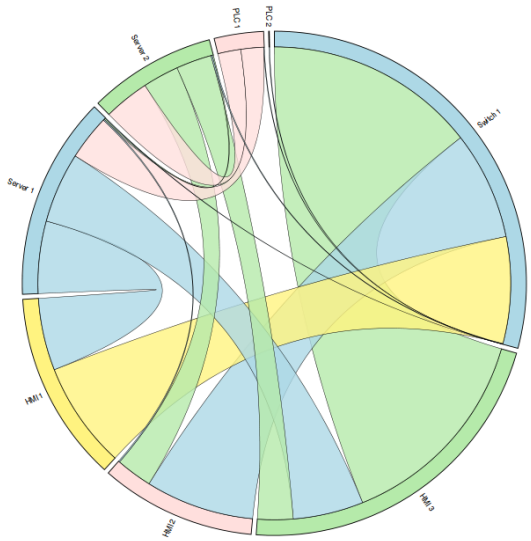


Fig. 2: Diagrama de cuerdas representando un conjunto de flujos de red legítimos.

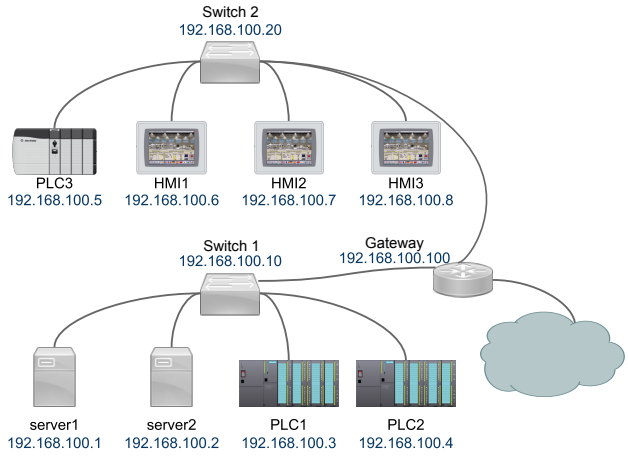


Fig. 4: Topología de red de la red industrial de prueba.

negro (ver figura 7). Además este tipo de flujos son los únicos en los que se utiliza la información de la lista blanca para representarlos, ya que en los datos recogidos no hay datos que impliquen a esos flujos.

IV. Applicación en una red industrial

Esta sección prueba la solución presentada anteriormente con datos reales de una red industrial.

A. *Red de prueba*

Realizar pruebas de seguridad en una red industrial real y en marcha puede ocasionar consecuencias inesperadas, como fallos en el funcionamiento de la red o situaciones potencialmente peligrosas [19]. Además de momento, no hay ningun conjunto de datos estándar con datos reales de flujo de una red industrial con varios dispositivos. Por ello, se ha duplicado la red de control de una instalación industrial real para realizar las pruebas en un entorno de laboratorio. La red original es la red de control de una línea de pintado de coches de una planta de fabricación.

La figura 4 muestra la topología de red de la red de prueba. Los switches son los dispositivos de red que envían los paquetes de flujo a los recolectores. En esta red se

utiliza NetFlow de Cisco, versión 5 para el envío de la información de flujo. Además el Switch 1 es además el servidor DNS de la red.

Hay tres controladores lógicos programables (PLCs) en la red, que son los responsables del control de proceso industrial. Dos servidores de control extraen la información del proceso a los tres PLCs simultáneamente. La comunicación entre los servidores y los controladores se realiza mediante el protocolo Modbus/TCP

También hay tres interfaces máquina-humano (HMIs) en la red, que permite que los operadores puedan supervisar el proceso y sus variables de una manera visual y accesible. HMI 1 recoge los datos del Servidor 1, el HMI 2, del Servidor 2 y, por último, el HMI 3 recoge datos de ambos servidores. La comunicación entre los HMIs y los servidores es mediante el protocolo OPC.

Una puerta de enlace o gateway conecta la red industrial con redes exteriores, donde se encuentra en este caso el recolector de flujos.

B. Implementación del sistema

Como se ha comentado, los flujos en el sistema de prueba son NetFlow versión 5. Los switches mandan los paquetes de flujo de red a agentes de Logstash[2] que, actuando como recolector de flujos, los recibe, los analiza y después los indexa en un cluster de ElasticSearch[3]. Este enfoque permite el uso de sistema de monitorización a gran escala y permite que las consultas se puedan realizar de manera rápida. El sistema de visualización que forma los diagramas de cuerdas ha sido desarrollado utilizando la librería D3 [20].

C. Anomalías de red

En esta sección se muestran diagramas de cuerdas en tres casos anómalos diferentes: un ataque de denegación de servicio (DoS), un escaneo de la red con el objetivo de enumerar los dispositivos presentes en la red y un fallo en la red donde un dispositivo deja de estar disponible. En estas pruebas todas las listas blancas y muestras de red han sido tomados en un periodo de diez minutos y con un umbral del 20% como variación máxima permitida en el número de paquetes registrados en un flujo.

C.1 Denegación de Servicio

Los ataques de denegación de servicio ocurren cuando un atacante intenta obstruir el funcionamiento real de un dispositivo o servicio dejándolo no disponible para los agentes legítimos. En redes industriales, donde la disponibilidad es el principal objetivo de la seguridad y donde problemas de latencia de red pueden crear problemas importantes de red, este tipo de ataques son muy peligrosos. En este caso, imitamos un ataque de denegación de servicio mediante el envío de grandes cantidades de paquetes ilegítimos del HMI 3 al Servidor 1.

El resultado de la visualización del ataque está en la figura 5. El flujo que muestra el ataque se muestra rellenado de color rojo, ya que aunque la comunicación entre ambos dispositivos está permitida, sobrepasa el número de paquetes permitidos. Al ser el número de paquetes enviados mayor, el HMI 3 ocupa una mayor sección del arco y la cuerda del flujo anómalo es más ancha en su lado.

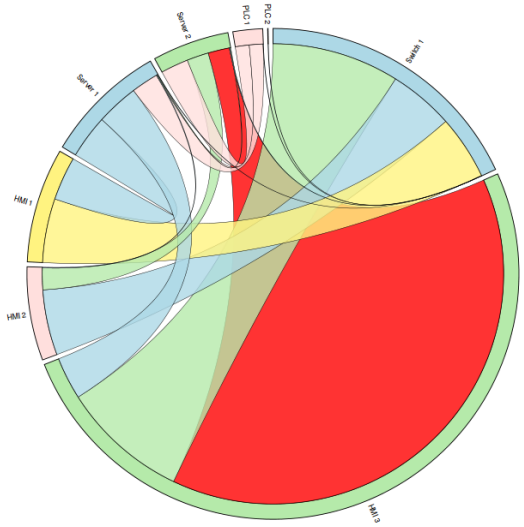


Fig. 5: Visualización de un ataque de denegación de servicio.

C.2 Descubrimiento de red

El descubrimiento de dispositivos es uno de los primeros pasos que un atacante ejecuta cuando obtiene acceso a una red desconocida para poder obtener información acerca de ella. El escaneo de puertos es una de las técnicas más utilizadas para el descubrimiento. En esta prueba se realiza un escaneo de puertos TCP Connect con Nmap desde el HMI 3.

La representación del ataque puede verse en la figura 6. Todos los flujos que incluyen a HMI 3 están marcados como anómalos, bien porque tiene prohibida la comunicación con la mayoría de hosts (p. ej. los PLCs) o porque utiliza puertos y/o protocolos diferentes para comunicarse con dispositivos con los que sí tiene permitida la comunicación.

C.3 Dispositivo no disponible

Por último, consideramos el caso donde un dispositivo tiene problemas de conectividad y no es capaz de comunicarse con la red y, por lo tanto, de enviar o recibir paquetes. Para la realización de esta prueba, se ha desconectado físicamente el Servidor 1 de la red.

La figura 7 muestra como los flujos del dispositivo caído han sido etiquetados como ausentes, y como tal, teñidos de negro. Para poder visualizar los datos de los flujos implicados, se han utilizado los datos registrados en la lista blanca.

V. Conclusiones y trabajos futuros

Hemos presentado un sistema para la monitorización de flujos de red que se vale de diagramas de cuerdas y listas blancas. Para ello, primero se elaboran una serie de listas

[2]https://github.com/elastic/logstash
[3]https://github.com/elastic/elasticsearch

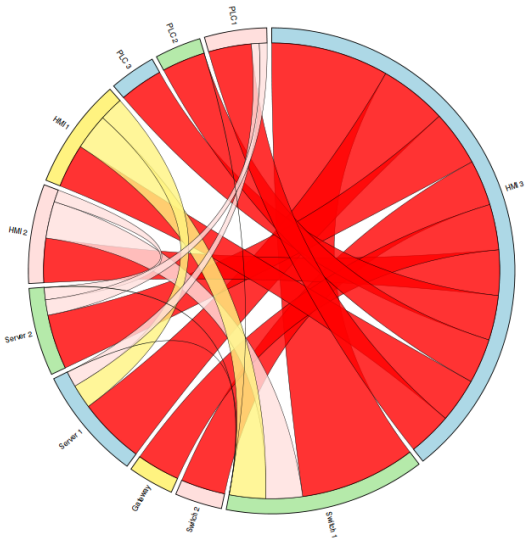


Fig. 6: Visualización de un escaneo de puertos.

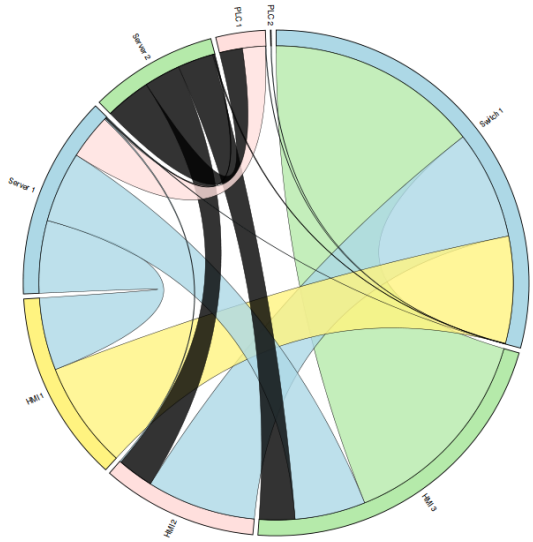


Fig. 7: Visualización de un dispositivo caído.

blancas temporales que tienen en cuenta el número de paquetes registrados, junto con las direcciones de red, puertos de servicio y protocolos IP que permite la detección de anomalías relacionadas con flujos de red. Todos los flujos se etiquetan utilizando la lista blanca como referencia (legítimo, anómalo, puerto o protocolo incorrecto, ausente y tamaño de flujo anómalo).

Estos datos etiquetados se utilizan para producir diagramas de cuerdas que representan relaciones de red entre dispositivos diferentes, en donde el número de paquetes de red es la principal métrica para producir el diagrama, especialmente para establecer el tamaño de las cuerdas. El sistema de etiquetado también tiene un código de colores que hacen que los flujos anómalos destaquen con colores diferentes (en rojo o negro) y también proporciona información acerca de la razón por la que el flujo ha sido etiquetado como no legítimo, tanto en la visualización como en las alertas lanzadas.

A. *Trabajos futuros*

La información relativa a los puertos y protocolos es utilizada para la detección de anomalías, pero en la visualización no muestra la información relativa a ellas. La inclusión de estas características aumentaría la cantidad de información que el operador recibe de manera visual, pero también aumenta el riesgo de complicar las visualizaciones demasiado, hasta el punto de no poder cumplir su cometido.

Las listas blancas se crean al principio de la recolección de flujos y no son directamente editables desde la interfaz visual. Sin embargo, es interesante ofrecer al usuario esta opción de editar las listas blancas para poder permitir flujos marcados como ilegítimos si el operador puede determinar su legitimidad y no ha sido detectado en la fase de aprendizaje.

Referencias

[1] A. Cárdenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems.," in *HotSec*, 2008.

[2] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security, Special publication 800-82," tech. rep., National Institute of Standards and Technology, June 2011.

[3] Consejo de la Unión Europea, "Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección," *Diario Oficial de la Unión Europea*, vol. L345, pp. 75–82, Diciembre 2008.

[4] B. Miller and D. Rowe, "A survey of SCADA and Critical Infrastructure incidents," in *Proceedings of the 1st Annual conference on Research in information technology*, pp. 51–56, ACM, 2012.

[5] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier," *White paper, Symantec Corp., Security Response*, 2011.

[6] McAfee, "Global Energy Cyberattacks: "Night Dragon" (white paper)," tech. rep., McAfee, 2011.

[7] D. Hentunen and A. Tikkanen, "Havex Hunts For ICS/SCADA Systems," June 2014. [Online]. Available: http://www.f-secure.com/weblog/archives/00002718.html (Retrieved: 2015-07-26).

[8] M. Cheminod, L. Durante, and A. Valenzano, "Review of Security Issues in Industrial Networks," *IEEE Transactions on Industrial Informatics*, vol. 9, no. 1, pp. 277–293, 2013.

[9] R. R. R. Barbosa, R. Sadre, and A. Pras, "Flow Whitelisting in SCADA Networks," *International Journal of Critical Infrastructure Protection*, vol. 6, no. 3, pp. 150–158, 2013.

[10] M. Herrero Collantes and A. López Padilla, "Protocolos y Seguridad de red en infraestructuras SCI," tech. rep., INCIBE: Instituto Nacional de Ciberseguridad, Mayo 2015.

[11] I. Garitano, M. Iturbe, I. Arenaza-Nuño, R. Uribeetxeberria, and U. Zurutuza, "Sistema de Detección de Anomalías para protocolos propietarios de Control Industrial," in *XIII Spanish Meeting on Cryptology and Information Security (RECSI 2014)*, (Alicante, Spain), pp. 315–320, University of Alicante, Sep 2014.

[12] M. Hoeve, "Detecting Intrusions in Encrypted Control Traffic," in *Proceedings of the First ACM Workshop on Smart Energy Grid Security*, SEGS '13, (New York, NY, USA), pp. 23–28, ACM, 2013.

[13] B. Genge, D. A. Rusu, and P. Haller, "A connection pattern-based approach to detect network traffic anomalies in critical infrastructures," in *Proceedings of the Seventh European Workshop on System Security*, (Amsterdam, Netherlands), ACM, 2014.

[14] M. Krzywinski, J. Schein, I. Birol, J. Connors, R. Gascoyne, D. Horsman, S. J. Jones, and M. A. Marra, "Circos: an information aesthetic for comparative genomics," *Genome Research*, vol. 19, no. 9, pp. 1639–1645, 2009.

[15] J. Mazel, R. Fontugne, and K. Fukuda, "Visual comparison of network anomaly detectors with chord diagrams," in *Proceed-*

ings of the 29th Annual ACM Symposium on Applied Computing, pp. 473–480, ACM, 2014.

[16] R. Layton, P. Watters, and R. Dazeley, "Unsupervised authorship analysis of phishing webpages," in *Communications and Information Technologies (ISCIT), 2012 International Symposium on*, pp. 1104–1109, IEEE, 2012.

[17] S. Chen, C. Guo, X. Yuan, F. Merkle, H. Schaefer, and T. Ertl, "OCEANS: online collaborative explorative analysis on network security," in *Proceedings of the Eleventh Workshop on Visualization for Cyber Security*, pp. 1–8, ACM, 2014.

[18] T. Tack, A. Maier, and O. Niggemann, "On Visual Analytics in Plant Monitoring," in *Informatics in Control, Automation and Robotics*, pp. 19–33, Springer, 2014.

[19] D. Duggan, M. Berg, J. Dillinger, and J. Stamp, "Penetration testing of industrial control systems," Tech. Rep. SAND2005-2846P, Sandia National Laboratories, March 2005.

[20] M. Bostock, V. Ogievetsky, and J. Heer, "D^3 data-driven documents," *Visualization and Computer Graphics, IEEE Transactions on*, vol. 17, no. 12, pp. 2301–2309, 2011.