Una arquitectura segregada para una empresa basada en la confianza Red de Internet de las Cosas

Davide Ferrarisa , Carmen Fernandez-Gagoa , Joshua Danielb , Javier Lopeza
aNICS Lab, Universidad de Málaga, 29071 Málaga,
España {ferraris,mcgago,jlm}
@lcc.uma.es bBritish Telecom,Orion Floor 5 pp10, Adastral Park, Martlesham Heath, IP5 3RE, Ipswich,
Inglaterra joshua.daniel@bt.com

Resumen—Con el número cada vez mayor de dispositivos domésticos inteligentes, los problemas relacionados con estos entornos también están creciendo. Con una superficie de ataque cada vez mayor, no existe una forma estándar de proteger los hogares y sus habitantes de nuevas amenazas. Los habitantes rara vez son conscientes de las crecientes amenazas a la seguridad a las que están expuestos y de cómo gestionarlas. Para abordar este problema proponemos una solución basada en arquitecturas segmentadas similares a las utilizadas en sistemas industriales. En este enfoque, la casa inteligente se segmenta en varios niveles, que en términos generales se pueden clasificar en un nivel interno y un nivel externo.
El nivel externo está protegido por un firewall que verifica la comunicación desde/hacia Internet hacia/desde los dispositivos externos.
El nivel interno está protegido por un firewall adicional que filtra la información y las comunicaciones entre los dispositivos externos e internos. Esta segmentación garantiza un entorno de confianza entre las entidades de la red interna. En este artículo, proponemos un modelo de confianza adaptativo que verifica el comportamiento de las entidades y, en caso de que las entidades violen las reglas de confianza, pueden ponerse en cuarentena o prohibirse de la red.

Términos del índice: seguridad, confianza, privacidad, Internet de las cosas (IoT), hogar inteligente

I. INTRODUCCIÓN

Ahora que el Internet de las cosas (IoT) permite hogares y ciudades inteligentes, ahora es posible conectar entidades cotidianas que se controlan de forma remota (es decir, mediante un teléfono inteligente). Para facilitar esta implementación, los fabricantes de dichos dispositivos permiten controlarlos desde un centro de comando basado en la nube, lo que permite a los propietarios controlarlos incluso cuando están lejos de su red doméstica. La funcionalidad también se ha ampliado para permitir que los dispositivos conectados se sincronicen y reciban instrucciones de otros dispositivos conectados. Los fabricantes de dispositivos inteligentes [1] y asistentes [2] pueden utilizar diferentes tecnologías de comunicación, como Zigbee o Zwave [20]. Estas tecnologías tienden a utilizar protocolos propietarios o uno de los muchos protocolos estándar [9] y no pueden comunicarse directamente entre sí [10].

Otro problema es el uso de diferentes versiones de una misma tecnología, en el caso de Bluetooth Low Energy (BLE), no siempre se garantiza la compatibilidad inversa con la versión anterior [4]. La solución para esto ha sido tradicionalmente que los fabricantes creen su propio centro de IoT que corresponda a los dispositivos que fabrican o pretenden admitir.

Considerando estos aspectos, los desafíos en la construcción de un conjunto Cada vez es más difícil que los objetos inteligentes cooperen entre sí. Ferraris et al. [8] proponen un marco para garantizar la confianza en el desarrollo de un objeto inteligente en todo el ciclo de vida del sistema. Además, este marco garantiza una planificación cuidadosa desde el punto de vista del desarrollador. Desde el punto de vista del cliente, sin planificación, es posible que un hogar termine con dispositivos de múltiples fabricantes, creando heterogeneidad. Además, con algunos centros de IoT correspondientes a sus respectivos dispositivos de IoT, la complejidad del sistema crece. Otros desafíos importantes en IoT son los relacionados con cuestiones de seguridad, confianza y privacidad. Estas amenazas pueden ser internas o externas de Internet y apuntar a las partes internas y más vulnerables del sistema. En cuanto al aspecto de seguridad, sin una arquitectura segura, IoT puede sufrir fallos de funcionamiento o ataques. Para evitar estos problemas, IoT necesita un enfoque holístico que asegure todos los elementos, desde la capa física hasta la de aplicación [22]. Estas cuestiones de seguridad son vitales para preservar la privacidad y construir una comunidad confiable de dispositivos.

Los usuarios consideran que la privacidad es muy importante [21] y la confianza es necesaria para permitir que las cosas inteligentes colaboren entre sí en un entorno dinámico y heterogéneo como el IoT sin comprometer la privacidad [7]. Según Moyano et al. [17], consideramos la confianza como "la expectativa personal, única y temporal que un fideicomitente deposita en un fiduciario con respecto al resultado de una interacción entre ellos".

En este artículo, proponemos una arquitectura para un entorno doméstico inteligente basada en arquitecturas industriales, donde las redes están separadas en diferentes niveles de red con diferentes controles de seguridad de red, como firewalls utilizados para segregar, detectar y proteger sistemas (como arquitecturas SCADA [3]). Hemos desarrollado un modelo de control de acceso adaptable basado en la confianza para garantizar que las relaciones de confianza coincidan en la arquitectura interna y externa.

La estructura del documento es la siguiente. En la Sección II describimos el trabajo relacionado. Luego la motivación se describe en la Sección III. En la Sección IV explicamos nuestra arquitectura propuesta y en la Sección V nuestro modelo de confianza adaptativa. Un escenario de caso de uso se describe en la Sección VI. Finalmente, en la Sección VII concluimos y discutimos el trabajo futuro.

II. TRABAJO RELACIONADO

El entorno de IoT es una red mundial de entidades interconectadas localizables, utilizables y legibles a través de la

1http://www2.meethue.com/en-gb/
2https://developer.amazon.com/alexa

Internet [22]. Se espera que estos objetos tengan que interactuar entre sí a menudo en condiciones de incertidumbre.
Se necesitan mecanismos para resolver esta falta de información y la confianza puede ayudar a abordar esta necesidad [28]. En relación con la confianza, la reputación es más objetiva y puede ser un parámetro para la decisión de confianza [13]. La heterogeneidad y dinamismo de IoT han planteado interrogantes y llevado a proponer algunas arquitecturas posibles. Romano y col. [23] identificaron cuatro arquitecturas principales, cada una de ellas tiene sus fortalezas y debilidades. Estas arquitecturas son IoT centralizada y colaborativa, Intranets de las cosas conectadas y distribuidas. En un enfoque centralizado, una puerta de enlace, como un centro de hogar inteligente, gestiona un grupo de dispositivos (en su mayoría pasivos), con la puerta de enlace de control principal y la lógica en el propio centro. El principal riesgo de esta arquitectura es que, cuando el centro inteligente se ve comprometido o no funciona correctamente, toda la arquitectura falla. Como afirma Singh [25], muchos de estos ataques se pueden realizar contra el centro de IoT doméstico. Un ataque de modificación de mensajes o un ataque de repetición son ejemplos de dos de estos ataques que pueden tener un impacto importante en un hogar inteligente. Con una señal repetida, el atacante puede repetir una orden indefinidamente. Por ejemplo, un atacante puede abrir y cerrar una ventana continuamente. Con un ataque de modificación de mensajes, el atacante puede cambiar un parámetro establecido por el usuario o por el sistema. En caso de incendio, por ejemplo, se puede modificar el umbral y provocar que la alarma se encienda demasiado tarde o quede apagada. Un problema como este es una gran amenaza no sólo para todos los que viven en esa casa sino también para sus vecinos. En un enfoque distribuido, todos los nodos tienen reglas determinantes [23]. Este modelo espera una entrada que, cuando cumple una condición, el dispositivo ejecuta una acción de forma local e independiente. En una red como ésta se espera mucha más comunicación entre pares [6].
Existen variaciones a este tipo de arquitectura, como la propuesta por Parra [19] donde algunos pares están en medio de la comunicación, por lo que si no cumplen con la garantía de confianza, la arquitectura también fallará. Otro gran problema con esta arquitectura es que los pares no están tan protegidos como el centro inteligente y, en este caso, puede ser más fácil comprometerlos. Según Román et al. [23], la vulnerabilidad de una arquitectura distribuida radica en el hecho de que los nodos no están tan protegidos como la unidad central. De hecho, si un atacante sabe cómo apuntar a un nodo en particular, puede, por ejemplo, filtrar información privada. Estas arquitecturas se utilizan como base para crear marcos utilizados en el campo de IoT [7], [26] y algunas de estas estructuras se aplican a muchos campos, como ciudades inteligentes, redes inteligentes o hogares inteligentes [19]. Algunas de estas arquitecturas se utilizan en sistemas industriales [27] donde las redes se dividen en dos o más partes, utilizando firewalls para segregar las redes más vulnerables y protegerlas del acceso directo a Internet. Este enfoque mejora la seguridad y la privacidad.
Son características fundamentales que deben garantizarse para proteger a los usuarios y las cosas de ataques o robo de información [21]. Para resolver los problemas de privacidad de IoT, un enfoque cada vez más importante es la Privacidad por Diseño (PbD), como se señala en el informe de la Comisión Federal de Comercio de EE. UU. (FTC) sobre la privacidad del consumidor [5].

En IoT, los desafíos con respecto a la privacidad se refieren principalmente a los usuarios y a cómo han almacenado sus datos privados en la arquitectura. Dependiendo de las aplicaciones utilizadas, las cuestiones de privacidad son muy diferentes entre sí [21]. La privacidad y la confianza están estrictamente relacionadas, Ferraris et al. [8] desarrolló un marco que garantiza la confianza en el desarrollo de una entidad de IoT. En este marco, los autores afirman que la confianza está fuertemente relacionada con la privacidad y otras propiedades de seguridad y en la fase de requisitos es posible vincular este tipo de requisitos entre sí para garantizar la trazabilidad. Aquí nos centramos más en la fase de necesidad y en su relación con la fase de utilización. También tomamos en consideración actividades transversales como el análisis de amenazas y riesgos. De hecho, otro desafío del IoT es proteger los entornos de diferentes ataques conocidos y desconocidos. Hu et al. [12] se centran en entornos de IoT relacionados con ataques. Afirman que ahora es más importante que nunca que las arquitecturas propuestas tengan en cuenta estos ataques y propongan soluciones a este problema. En nuestro trabajo, proponemos una arquitectura que puede prevenir este tipo de ataques, como se demuestra en las siguientes secciones.

III. MOTIVACIÓN

En un sistema industrial, la idea es definir y crear límites fijos entre redes para hacer el sistema menos vulnerable y reducir la posibilidad de ataques realizados por agentes externos maliciosos [18]. En un entorno doméstico inteligente, los consumidores finales no anticipan estos límites, por lo que las arquitecturas típicas están centralizadas o distribuidas [19]. Los límites estrictos no están definidos por las diversas redes internas ni por las redes externas.

Un camino a seguir para resolver este dilema arquitectónico es aplicar la arquitectura de sistemas industriales a un entorno doméstico inteligente. Esto permitiría una segmentación clara de la red y la inyección de controles de seguridad, como firewalls en las interfaces y un sistema tipo SCADA para proteger los dispositivos domésticos que están conectados directamente a Internet. Los riesgos más comunes de estas arquitecturas de hogares inteligentes son los riesgos cibernéticos (es decir, ransomware, malware) y riesgos físicos (es decir, incendio, robo). Las causas de estos riesgos pueden ser ataques de día cero en los que los atacantes utilizan Phishing o Spear-phishing para dirigirse al consumidor final. Este tipo de ataques, que invaden las redes, están actualmente en aumento debido al mayor impacto [14] de cargas útiles como Wannacry [16]. Sin embargo, la manipulación de estos sistemas críticos conectados a Internet en el hogar puede tener graves consecuencias que pueden llegar hasta la muerte (ataque a la vigilancia de la salud) [11]. Una consideración práctica necesaria reside en la segmentación de la red entre los objetos inteligentes, los centros inteligentes, Internet y la red utilizada por el consumidor para funciones críticas como la banca. Este tipo de conexión representa un riesgo importante y se necesita protección para dividir la red interna en partes para proteger el nivel interno [27].
También se necesitan subredes de red, sistemas de detección y prevención de intrusiones, firewalls y otros controles de seguridad similares para proteger y monitorear la red, y permitir que solo puertos específicos realicen las acciones necesarias.

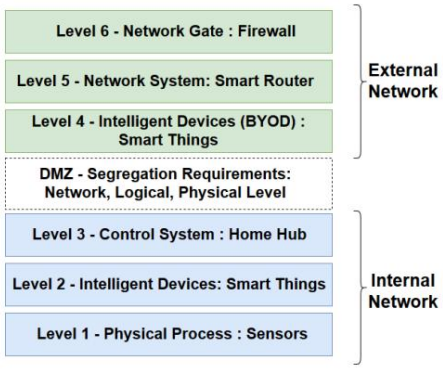

Fig. 1. Niveles de jerarquía de la arquitectura segregada

En este artículo, proponemos una arquitectura que garantiza un entorno confiable segregado donde el intercambio de información/lógica con múltiples centros podría almacenarse y procesarse de manera confiable. Esta es una nueva forma de intentar resolver los principales problemas de seguridad, confianza y privacidad relacionados con las arquitecturas clásicas de IoT [24].

IV. ARQUITECTURA

El principal objetivo de este documento es proteger las entidades de IoT mediante una arquitectura de confianza segregada. Por confianza segregada queremos decir que las entidades de IoT dentro de la red interna pueden confiar en las entidades con las que se les permite interactuar.

Esta segregación está garantizada por la arquitectura interna, que está diseñada para prevenir amenazas externas e internas. Esta arquitectura es similar a la obra de Obregón [18]. Más allá de este trabajo, hemos desarrollado el modelo que se muestra en la Figura 1, que se divide en seis niveles más una Zona Desmilitarizada (DMZ). Podemos ver que los niveles se agrupan principalmente en dos zonas: la zona azul está relacionada con la red interna y la zona verde está relacionada con la red externa.

Empezando desde abajo, el primer nivel se refiere a los procesos físicos. En un entorno doméstico inteligente, este nivel comprende los sensores, que recopilan datos sin procesar del campo y los envían al nivel superior, donde se encuentran los dispositivos o cosas inteligentes. Estos dispositivos deben procesar y analizar los datos brutos originados en los sensores y, cuando sea necesario, actuar.
Por ejemplo, un sensor de humo inteligente puede detectar humo y, si supera un umbral, el sensor activa la alarma de humo.
El tercer nivel es para el sistema de control, donde hay una unidad central (como un centro doméstico) que tiene que monitorear los otros objetos inteligentes y ser el puente entre ellos y los niveles superiores e Internet. La primera segregación tiene lugar en este nivel. Este nivel es el más alto de la zona inferior. El centro doméstico está conectado a Internet a través de una DMZ. Esta zona evita que el nivel inferior se vea comprometido por amenazas externas y un firewall monitorea el tráfico entrante y saliente. Esta DMZ debe satisfacer los requisitos de segregación para los niveles de red, lógico y físico.

El firewall permite el tráfico desde la DMZ a la red interna. Esta configuración puede proteger la red interna de amenazas externas, preservando la privacidad al proteger los datos almacenados dentro de la zona protegida y garantizando zonas confiables para el intercambio de información y datos cuando sea necesario. Para Por ejemplo, cuando una parte de la casa está físicamente comprometida, es posible transferir los datos a otra área segura.

Más allá de la zona interior, hay un cuarto nivel. En este nivel tenemos todas las entidades clasificadas bajo el paradigma Bring Your Own Device (BYOD) [15]. Estos dispositivos son, por ejemplo, teléfonos inteligentes o portátiles que el propietario puede llevar consigo en redes externas. Por este motivo, tienen que estar segregados de la red interna pero pueden comunicarse con ella a través de la DMZ.

Luego tenemos el nivel cinco y está relacionado con el Sistema de Red, que se comunica con Internet a través del nivel superior. En este nivel tenemos el router inteligente que podría bloquear algunas comunicaciones o reenviarlas a la capa inferior (en el caso de que provenga de Internet) o a la capa de arriba (en el caso de que provenga del nivel 4). Finalmente está el sexto nivel donde podemos encontrar el firewall, protegiendo la capa externa de las amenazas de Internet. Tanto el firewall como el router inteligente de capa cinco se pueden implementar para dejar pasar o bloquear la comunicación en ambas direcciones. Esta implementación depende en gran medida del contexto y el entorno.

V. MODELO DE CONFIANZA ADAPTABLE

El modelo de confianza adaptativa funciona en diferentes situaciones. Según Ferraris et al. [8], durante la fase de utilización, una entidad puede unirse, permanecer o abandonar una red. Para las acciones de unirse y permanecer, se debe calcular una estimación de confianza. El nivel de confianza calculado será fundamental para permitir que la nueva entidad se una o permanezca en la red. El smart hub es el dispositivo que calculará los valores y tiene derechos de acceso a las bases de datos (DB). Podría almacenar información relacionada con las acciones realizadas por las entidades con fines forenses (pero esto está fuera del alcance del artículo). Asumimos que Smart Hub no puede verse comprometido porque tiene una raíz de confianza3 .

A. Estimación de confianza

En nuestro modelo, la estimación de la confianza es central y se realiza con diferentes criterios. Se hace para decidir si una nueva entidad puede unirse a la red y para decidir si una entidad puede permanecer en la parte interna o externa de la red. Los criterios que se tienen en cuenta son: base de datos de reputación, base de datos de amenazas, cálculo de riesgos y base de datos de amenazas

de contexto. En esta base de datos se recopilan las vulnerabilidades conocidas de los dispositivos inteligentes. En el caso de que no se conozcan ataques relacionados con el dispositivo, su valor de confianza es mayor. En el caso de ataques conocidos, cuanto mayor es el peligro, menor es el valor de confianza.

Base de datos de reputación. La base de datos de reputación se utiliza para almacenar los valores de reputación antiguos de los dispositivos. Por ejemplo, en el caso de que un nuevo dispositivo intente unirse a la red nuevamente, pero en el pasado ha sido prohibido, el centro inteligente denegará su acceso. Asumimos que una prohibición se realiza sólo después de un problema de seguridad grave; por esta razón, un dispositivo prohibido no puede volver a unirse a la red. Además, evitando una segunda oportunidad prevenimos los Ataques de Blanqueo (WA). Suponemos que ambas bases de datos están protegidas y cifradas. Además, se almacenan en

3https://www.synopsys.com/designware-ip/technical-bulletin/secure-iot-system.html

la red interna donde asumimos que una entidad maliciosa no puede acceder debido a la implementación de las fases de unirse, permanecer y salir (como mostraremos más adelante).

Contexto. El contexto depende del entorno, del propósito y de los servicios que el dispositivo proporciona solo o con otros dispositivos inteligentes. Cuanto más importante sea un dispositivo, mayor será el nivel de confianza necesario.

Cálculo de Riesgos. El riesgo puede ser provocado por ataques, fallas del sistema, agregar o cambiar dispositivos. En el estado del arte existen multitud de técnicas relacionadas con la estimación de riesgos [2]. Consideramos tres parámetros para calcular el riesgo. El primer parámetro es la probabilidad (L) de un evento; esta es la probabilidad de que pueda ocurrir una situación que perjudique al sistema (ya sea un ataque o un mal funcionamiento). El segundo parámetro es la gravedad (S) del efecto que un mal funcionamiento o un ataque puede tener en el sistema; cuanto más crítico sea el componente involucrado, más crítica será la amenaza para todo el sistema.
Finalmente, hay un parámetro que normalmente no se tiene en cuenta pero que creemos que es crucial para calcular el riesgo: la detectabilidad (D). La detectabilidad es la posibilidad de que se produzca un mal funcionamiento o que se pueda detectar un dispositivo infectado. Si una Si se produce un ataque y no podemos detectarlo, el sistema fallará o será manipulado. Hemos considerado la detectabilidad y la probabilidad por separado porque la probabilidad está relacionada únicamente con la probabilidad de que ocurra un evento, incluso si lo detectamos o no. Como se muestra en las Tablas I, II y III los valores de riesgo tienen diferentes significados según su tipología.

TABLA I
PROBABILIDAD

Valor	Significado
Bajo (1)	Es poco probable que el evento suceda
Medio (3)	Es muy probable que el evento suceda.
Alto (9)	Es casi seguro que el evento sucederá.

TABLA II
GRAVEDAD

Valor	Significado
Bajo (1)	La red no está dañada.
Medio (3)	La red puede estar parcialmente dañada.
Alto (9)	La red puede volverse completamente inútil

TABLA III
DETECTABILIDAD

Valor	Significado
Bajo (1)	El problema es fácilmente detectable.
Medio (3)	El problema no se puede detectar por completo
Alto (9)	No es posible detectar el problema.

Hemos considerado solo tres valores para cada parámetro para simplificar el cálculo. Los valores se combinan entre ellos mediante una multiplicación. Este es un enfoque común utilizado en muchos métodos de riesgo [2]. Si el resultado es inferior a 9, tenemos un riesgo bajo. Si el resultado está entre 9 y 27, tenemos un riesgo medio. Si el valor es superior a 27, tenemos un riesgo alto. El valor del riesgo global se ha elegido según los siguientes criterios:

1) Es el mismo nivel de todos los parámetros si pertenecen al mismo nivel (es decir, bajo si L, S y D son bajos).
2) Bajo, si solo hay un parámetro medio y los otros dos parámetros son bajos.
3) Alto, si hay dos o más parámetros configurados en alto o dos parámetros configurados en medio y uno configurado en alto.
4) Medio, en caso contrario.

En el caso de que el riesgo calculado sea alto, el dispositivo no se podrá agregar a la red o se deberá prohibir. En el caso de que el valor del riesgo sea bajo o medio el dispositivo puede unirse o permanecer en la red dependiendo de otros criterios.

B. Únete, quédate y vete

Unirse. Cuando el propietario de una casa inteligente permite que una nueva entidad se conecte a la red, se comunica con el monitor centralizado (es decir, un centro inteligente) y solicita unirse a la red y a las otras entidades. El centro inteligente verifica los derechos de la entidad (es decir, propietario, contraseña, cálculo de riesgo), le indica cómo unirse a las otras entidades y le proporciona la clave adecuada para intercambiar mensajes. La regla para unirse a una entidad depende de la estimación de confianza. La decisión de la red se basa en si la nueva entidad es BYOD o no. Si es BYOD, la nueva entidad solo puede unirse a la red externa. El procedimiento de unión es similar a la técnica SDP4. Cuando el nuevo dispositivo se une a la red, envía un mensaje de difusión para comunicarse con el centro inteligente y solicita permiso para unirse a la red (acción 1). El centro inteligente verifica los permisos del nuevo dispositivo (es decir, contraseña, clave de propietario, derechos) y toma la decisión de unirse.
Si se deniega el acceso a la red, el centro inteligente indica al nuevo dispositivo que no puede unirse a la red. Si se concede el acceso, el centro inteligente le indica al nuevo dispositivo que puede unirse a la red y con qué otros dispositivos puede interactuar (acción 2). Posteriormente, el smart hub informa a los dispositivos ya presentes en la red que pueden interactuar con el nuevo dispositivo (acción 3). En ambas acciones 2 y 3, el hub inteligente proporciona una clave simétrica al dispositivo permitido y a los dispositivos ya presentes en la red para permitir la comunicación entre ellos. Los dispositivos deben reconocer el smart hub y, a partir de ese momento, puede comenzar la interacción entre los dispositivos.

Permanecer. Cuando una entidad permanece en una red, debe ser monitoreada, según factores externos e internos. Durante el seguimiento, el centro inteligente comprueba si las entidades se comportan con normalidad. Si ocurre algo inesperado (según el contexto, el cálculo del riesgo y la entidad involucrada), se necesita una estimación de confianza para decidir si la entidad se está comportando maliciosamente o no. Durante la estimación de confianza se tienen en cuenta el contexto y el cálculo de riesgo de la acción, junto con los datos de la base de datos de reputación donde se almacena el historial de las entidades y una base de datos de amenazas actualizada con los últimos ataques conocidos. El centro inteligente puede permitir que la entidad permanezca o puede decidir prohibirla o ponerla en cuarentena. Cuando una entidad es puesta en cuarentena, permanece en la red sin poder comunicarse con la otra.

4https://cloudsecurityalliance.org/download/software-defined-perimeter/

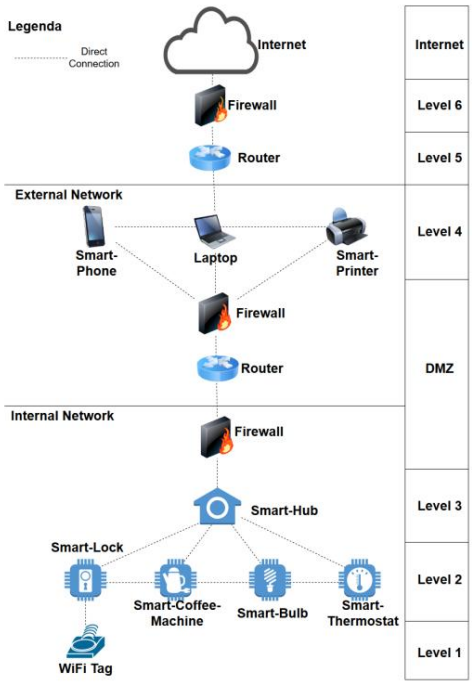

Fig. 2. Hogar inteligente: arquitectura de confianza segregada

entidades. La entidad sólo puede recibir comunicaciones del centro inteligente. La cuarentena continuará hasta que haya nueva información disponible (es decir, ataques conocidos o vulnerabilidades relacionadas con la entidad). En caso de que una entidad sea prohibida o puesta en cuarentena, el centro inteligente debe comunicar la decisión a las entidades.

tener una conexión con el prohibido. El modelo para la decisión de estancia es similar al trabajo de Atlam et al. [1]. Han propuesto un modelo de control de acceso basado en riesgos para IoT para calcular el riesgo asociado con la solicitud de acceso a un recurso en particular. Ampliamos este modelo utilizando el cálculo de riesgo como parámetro para la estimación de confianza.

Dejar. Cuando una entidad abandona la red interna o externa, debe anunciar su intención de salir al centro inteligente y a las entidades relacionadas. Para mejorar la seguridad, el centro inteligente debe comunicar el cambio a sus entidades relacionadas.

VI. ESCENARIO DE CASA INTELIGENTE

La arquitectura de la casa inteligente se muestra en la Figura 2. En el lado derecho de la figura se encuentran los niveles relacionados con la Figura 1. Como se puede observar, está compuesta por dos redes: una interna y otra externa. La red interna comprende una cerradura inteligente, una cafetera inteligente, una bombilla inteligente y un termostato inteligente. Estas entidades sólo pueden comunicarse con otra entidad según su propósito. El enlace para la comunicación está representado por las líneas de puntos en la Figura 2.

La cerradura inteligente no tiene ninguna conexión con la cafetera inteligente porque no hay motivo para que se comuniquen directamente entre sí. Por el contrario, la bombilla inteligente puede recibir información de la cerradura inteligente. De hecho, cuando se abre la puerta, la cerradura inteligente envía una señal a la bombilla inteligente para encender las luces (en caso de que sea de noche). Todos estos dispositivos se comunican directamente con el centro inteligente, que monitorea sus actividades, permitiéndoles comunicarse directamente solo para propósitos determinados. La red interna está separada.

desde la red externa que contiene un teléfono inteligente, una computadora portátil y una impresora inteligente. Estos tres objetos pertenecen al paradigma BYOD. No pueden unirse a la red interna porque pueden unirse a otras redes y verse comprometidos. Supongamos que el propietario necesita una nueva cerradura inteligente y un teléfono inteligente.

A. Bloqueo inteligente

Cuando la cerradura inteligente se une a la red, se envía un mensaje de difusión a todos los dispositivos de la red. Los dispositivos inteligentes no reconocen el ID del nuevo dispositivo y no pueden responder. El centro inteligente reconoce el objeto como perteneciente al propietario de la casa inteligente; de hecho, asumimos que antes de unirse a una red, el propietario de la casa inteligente valida los dispositivos. Después de este mensaje, el centro inteligente inicia la estimación de confianza. El smart hub comprueba la base de datos de reputación para ver si la cerradura inteligente ha formado parte de la red anteriormente, aunque asumimos que el dispositivo es completamente nuevo. Se verifica la base de datos de amenazas para encontrar vulnerabilidades conocidas con respecto al modelo de cerradura inteligente y encuentra una vulnerabilidad conocida. El cálculo del riesgo tiene en cuenta los parámetros L, S y D. Para L, el centro inteligente decide asignar un valor medio porque la vulnerabilidad conocida podría explotarse. En cuanto al parámetro S, el smart hub decide dar un valor alto porque en caso de mal funcionamiento o ataques la cerradura inteligente pierde completamente sus funcionalidades. Finalmente, el valor D es bajo porque el proveedor ha diseñado la cerradura inteligente para proporcionar información sobre su funcionalidad. En resumen, tenemos un valor alto para S (9), un valor medio para L (3) y un valor bajo para D (1). Según estos valores, la estimación global del riesgo es media (27). Finalmente, el centro inteligente comprueba el contexto del dispositivo. El contexto está relacionado con la cooperación de la cerradura con la bombilla inteligente, por lo que en caso de que muestre un comportamiento malicioso o sufra un mal funcionamiento por parte de la cerradura, la bombilla inteligente también puede verse afectada. Además, la cerradura inteligente es de vital importancia para el entorno doméstico inteligente porque, en caso de comportamiento malicioso, puede permitir que extraños entren a la casa o puede impedir la entrada al propietario. La estimación de confianza toma en consideración los siguientes parámetros: el valor del riesgo es medio, la cooperación con la bombilla inteligente y el (Contexto) y la vulnerabilidad conocida encontrada en la base de datos de amenazas. Después de la estimación de confianza, el centro inteligente decide no permitir que la cerradura inteligente se una a la red. Esta acción de denegación protege a las entidades internas de ser amenazadas por el nuevo dispositivo y mantiene el nivel de confianza en la red interna.

B. Teléfono inteligente

El segundo dispositivo adquirido por el propietario es un teléfono inteligente. El dispositivo nunca antes se había unido a la red, por lo que la base de datos de reputación no tiene datos para él. La base de datos de amenazas no tiene ataques conocidos relacionados con el modelo y la versión del teléfono inteligente. El valor de riesgo se calcula como bajo (3) porque los parámetros L y D se consideran bajos (1) y el parámetro S se considera medio (3) porque en caso de mal funcionamiento o actividad maliciosa la red puede dañarse parcialmente. El contexto está relacionado con todos los dispositivos que pertenecen a la red externa y el centro inteligente de la red interna porque. Finalmente,

pertenece al paradigma BYOD por lo que en caso de aceptación sólo se permitirá unirse a la red externa. Una vez considerados todos estos parámetros, se permite que el teléfono inteligente se una a la red externa y se monitorea su comportamiento para anticipar posibles amenazas. Supongamos que después de unas semanas, el teléfono inteligente ha sido manipulado por una entidad maliciosa e intenta comunicarse con otras entidades inteligentes para controlarlas. La arquitectura permite que el teléfono inteligente pase a través del centro inteligente para comunicarse con las entidades inteligentes en la red interna. Suponemos que el teléfono inteligente envía repetidamente un comando a la bombilla inteligente para encender y apagar las luces cada cinco segundos. El centro inteligente detecta este comportamiento anormal y, utilizando el modelo adaptativo, decide bloquear las comunicaciones pertenecientes al teléfono inteligente y ponerlo en cuarentena. El centro inteligente, al comprobar la base de datos de amenazas, reconoce que el teléfono inteligente ha llevado a cabo un ataque de repetición. La base de datos de reputación se establece con un valor bajo y se notifica el evento al propietario de la casa inteligente.

Para concluir, hemos mostrado dos escenarios relacionados con un entorno doméstico inteligente. La arquitectura propuesta puede aumentar el nivel de seguridad de los hogares inteligentes y puede notificar a los propietarios si una entidad inteligente ha sido comprometida o si una entidad inteligente no puede unirse a la red por razones de seguridad.

VII. CONCLUSIONES Y TRABAJO FUTURO

Hemos propuesto una arquitectura de confianza segregada y un modelo de control de acceso adaptable basado en la confianza. La arquitectura consta de dos capas. La capa interna contiene entidades estáticas y tiene una mayor protección. La capa externa contiene entidades que pertenecen al paradigma BYOD. Esta capa también está protegida y puede comunicarse con la capa interna a través de un centro inteligente central. De acuerdo con esta arquitectura, hemos propuesto un modelo que monitorea el comportamiento de las entidades y los pasos que una entidad debe seguir cuando se une y sale de una red. Finalmente, existe un control de comportamiento para decidir si una entidad puede permanecer en la red interna o externa.

Para trabajos futuros, validaremos esta arquitectura y probaremos este entorno en una casa inteligente real, ampliaremos los casos de uso con más entidades y también insertaremos otros dispositivos invitados. Además, ampliaremos los valores de riesgo para tener más niveles de riesgo. También probaremos la arquitectura contra ataques conocidos. Además, nos centraremos más en la función de usabilidad considerando la posibilidad de que el centro inteligente niegue el acceso a dispositivos no maliciosos. En este caso diseñaremos el sistema para informar al propietario sobre este evento.

RECONOCIMIENTO

Este proyecto ha recibido financiación del programa de investigación e innovación Horizonte 2020 de la Unión Europea en virtud del acuerdo de subvención Marie Sklodowska-Curie nº 675320. Este trabajo refleja únicamente la opinión de los autores y la Agencia Ejecutiva de Investigación no es responsable del uso que pueda hacerse de la información que contiene.

REFERENCIAS

[1] Atlam, HF, Alenezi, A., Walters, RJ, Wills, GB, Daniel, J.: Desarrollo de un modelo de control de acceso adaptativo basado en riesgos para Internet de las cosas (2017)

[2] Behnia, A., Rashid, RA, Chaudhry, JA: Una encuesta sobre métodos de análisis de riesgos de seguridad de la información. SmartCR 2(1), 79–94 (2012)

[3] Boyer, SA: SCADA: supervisión, control y adquisición de datos. Interna- Sociedad Nacional de Automatización (2009)

[4] Bronzi, W., Frank, R., Castignani, G., Engel, T.: Análisis de robustez y rendimiento de baja energía de Bluetooth para comunicaciones entre vehículos. Redes ad hoc 37, 76–86 (2016)

[5] Comisión, UFT, et al.: Protección de la privacidad del consumidor en una era de cambios rápidos: recomendaciones para empresas y responsables políticos. Informe de la FTC (2012)

[6] Dohr, A., Modre-Opsrian, R., Drobics, M., Hayn, D., Schreier, G.: El Internet de las cosas para una vida asistida por ambiente. En: Tecnología de la información: Nuevas Generaciones (ITNG), 2010 Séptima Conferencia Internacional sobre. págs. 804–809. Es decir (2010)

[7] Fernández-Gago, C., Moyano, F., López, J.: Modelado de dinámicas de confianza en Internet de las cosas. Ciencias de la Información 396, 72–82 (2017)

[8] Ferraris, D., Fernández-Gago, C., López, J.: Un marco de confianza por diseño para Internet de las cosas. En: NTMS'2018 - Seguimiento de seguridad (NTMS 2018 Security Track). París, Francia (febrero de 2018)

[9] Gazis, V.: Un estudio de estándares para máquina a máquina e Internet de las cosas. Encuestas y tutoriales de comunicaciones del IEEE 19(1), 482–511 (2017)

[10] Gill, K., Yang, SH, Yao, F., Lu, X.: Un sistema de automatización del hogar basado en zigbee. Transacciones IEEE sobre electrónica de consumo 55(2) (2009)

[11] Hei, X., Du, X., Lin, S., Lee, I.: Pipac: esquema de control de acceso basado en patrón de infusión del paciente para un sistema inalámbrico de bomba de insulina. En: INFOCOM, Actas de 2013 IEEE. págs. 3030–3038. IEEE (2013)

[12] Hu, F.: Seguridad y privacidad en Internet de las cosas (IoT): modelos, algoritmos e implementaciones. Prensa CRC (2016)

[13] Jøsang, A., Ismail, R., Boyd, C.: Una encuesta sobre sistemas de confianza y reputación para la prestación de servicios en línea. Sistemas de apoyo a las decisiones 43(2), 618–644 (2007)

[14] Martin, G., Kinross, J., Hankin, C.: La ciberseguridad eficaz es fundamental para la seguridad del paciente (2017)

[15] Miller, KW, Voas, J., Hurlburt, GF: Byod: Consideraciones de seguridad y privacidad. Es profesional 14 (5), 53–55 (2012)

[16] Mohurle, S., Patil, M.: Un breve estudio de la amenaza de WannaCry: ataque de ransomware 2017. International Journal 8(5) (2017)

[17] Moyano, F., Fernández-Gago, C., López, J.: Un marco conceptual para modelos de confianza. En: Novena Conferencia Internacional sobre Confianza, Privacidad y Seguridad en los Negocios Digitales (TrustBus 2012. vol. 7449 de Lectures Notes in Computer Science, págs. 93-104. Springer Verlag (septiembre de 2012)

[18] Obregón, L.: Arquitectura segura para sistemas de control industrial. SANS Sala de lectura del Instituto InfoSec (2015)

[19] Parra, J., Hossain, MA, Uribarren, A., Jacob, E., El Saddik, A.: Arquitectura de hogar inteligente flexible que utiliza el perfil del dispositivo para servicios web: un enfoque de igual a igual. Revista internacional de hogares inteligentes 3 (2), 39–56 (2009)

[20] Pei, Z., Deng, Z., Yang, B., Cheng, X.: Protocolos de comunicación de redes de sensores inalámbricos orientados a aplicaciones y plataformas de hardware: una encuesta. En: Tecnología Industrial, 2008. ICIT 2008. Conferencia Internacional IEEE sobre. págs. 1–6. IEEE (2008)

[21] Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., Vasilakos, AV: La búsqueda de la privacidad en Internet de las cosas. Computación en la nube IEEE 3 (2), 36–45 (2016)

[22] Román, R., Nájera, P., López, J.: Asegurar el Internet de las cosas. Computadora 44 (9), 51–58 (2011)

[23] Roman, R., Zhou, J., Lopez, J.: Sobre las características y desafíos de la seguridad y la privacidad en la Internet distribuida de las cosas. Redes de computadoras 57 (10), 2266–2279 (2013)

[24] Singh, D., Tripathi, G., Jara, AJ: Un estudio sobre Internet de las cosas: visión de futuro, arquitectura, desafíos y servicios. En: Internet de las cosas (WF-IoT), foro mundial IEEE 2014 en. págs. 287–292. IEEE (2014)

[25] Singh, S., Sharma, PK, Park, JH: Sh-secnet: una arquitectura de red segura mejorada para el diagnóstico de amenazas a la seguridad en un hogar inteligente. Sostenibilidad 9(4), 513 (2017)

[26] Stojkoska, BLR, Trivodaliev, KV: Una revisión del Internet de las cosas para el hogar inteligente: desafíos y soluciones. Revista de Producción Más Limpia 140, 1454–1464 (2017)

[27] Stouffer, K., Falco, J., Scarone, K.: Guía para la seguridad de los sistemas de control industrial (ICS). Publicación especial del NIST 800(82), 16–16 (2011)

[28] Yan, Z., Zhang, P., Vasilakos, AV: Una encuesta sobre gestión de confianza para Internet de las cosas. Revista de aplicaciones informáticas y de redes 42, 120-134 (2014)