30/04/15

NOTA DE FUTURO 2015

WIND

LA SEGURIDAD EN EL INTERNET DE LAS COSAS

CENTRO DE ANÁLISIS Y PROSPECTIVA
GABINETE TÉCNICO DE LA GUARDIA CIVIL

Lecciones del pasado para el futuro conectado

A pesar de que ha estado con nosotros de alguna forma y bajo diferentes nombres durante muchos años, el Internet de las Cosas (IoT) de repente se ha convertido en la "cosa". La capacidad de conectarse, comunicarse y gestionar de forma remota un incalculable número de dispositivos conectados en red y automatizados a través de Internet se está convirtiendo en algo omnipresente, desde la planta de una fábrica a la sala de operaciones de un hospital o un sótano residencial.

La transición de las redes cerradas a las redes de las Tecnologías de la Información (TIs) de las empresas y al Internet público está creciendo a un ritmo alarmante, por lo que se han elevado las alarmas sobre la seguridad. Mientras nos hacemos cada vez más dependientes de los dispositivos inteligentes, interconectados en cada aspecto de nuestras vidas, ¿cómo los protegemos de las intrusiones y las interferencias que puedan comprometer la privacidad personal o amenazar la seguridad pública?

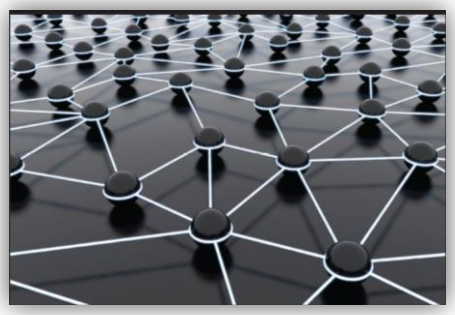
Como líder mundial en soluciones tecnológicas integradas, Wind River ha estado profundamente involucrado desde sus inicios con los dispositivos que realizan funciones críticas para la vida y que cumplen con los estrictos requisitos regulatorios. Este artículo examina las limitaciones y desafíos de seguridad planteados por los dispositivos conectados del IoT y el enfoque de Wind River para abordarlos.

En busca de la bala de plata

Los usuarios del IoT son muy conscientes de que la seguridad es primordial para el funcionamiento seguro y fiable de los dispositivos conectados. Es, de hecho, el habilitador fundamental del IoT.

Cuanto menor consenso haya mejor será la manera de implementar la seguridad en el IoT a nivel de dispositivo, de red y del sistema. Los cortafuegos y protocolos de red pueden gestionar el tráfico de alto nivel que transcurre a través de Internet, pero ¿cómo nos protegemos profundamente de los dispositivos de punto final incrustados, que por lo general tienen una misión muy específica, con los limitados recursos disponibles para lograrlo? Dada la novedad del Internet de las Cosas y el ritmo de la innovación hoy en día, parece que hay una expectativa general de algo totalmente nuevo, una revolucionaria solución de seguridad que surgirá y se adaptará de forma única al IoT.

Desafortunadamente, no existe una "bala de plata" que pueda mitigar eficazmente cualquier posible amenaza cibernética. La buena noticia, sin embargo, es que los controles de seguridad de las Tecnologías de la Información que han evolucionado a lo largo de los últimos 25 años pueden ser eficaces en el IoT. Podemos adaptarlos a las restricciones únicas de los dispositivos incrustados que integrarán cada vez más las redes del futuro.

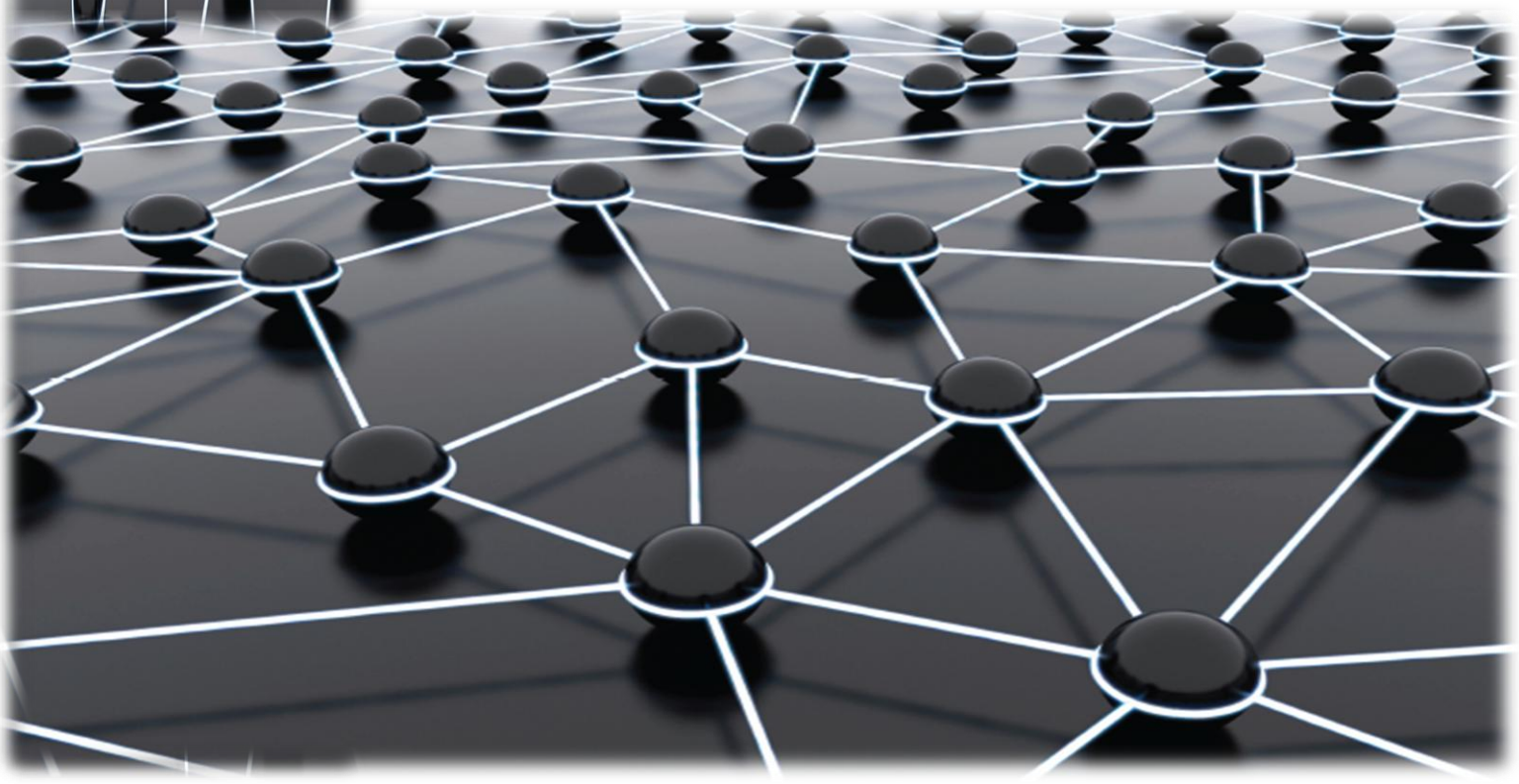


Cómo llegamos aquí:
La evolución de la seguridad de la red

La protección de datos ha sido un problema desde que los dos primeros ordenadores se conectaron entre sí. Con la comercialización de Internet, los problemas de seguridad para cubrir la intimidad personal, las transacciones financieras y la amenaza de un robo cibernético son más amplios. Ya sea accidental o maliciosa, la interferencia con los mandos de un marcapasos, un coche o un reactor nuclear es una amenaza para la vida humana.

Los controles de seguridad han evolucionado en paralelo a la evolución de la red, desde los primeros cortafuegos a finales de 1980 a protocolos más sofisticados, cortafuegos de aplicación consciente con detección de intrusos y sistemas de prevención (IDS / IPS), y con solución de incidentes de seguridad y gestión de eventos (SIEM). Estos controles intentaban mantener la actividad maliciosa fuera de las redes corporativas y detectar si lo hacían para obtener acceso. Si el malware lograba romper un cortafuegos, las técnicas de antivirus y las listas negras (blacklists) entraban en juego para identificar y solucionar el problema.

Más tarde, cuando el universo del malware se expandió y las actuaciones para evitar su detección avanzaron, las técnicas de listas blancas (whitelists) comenzaron a reemplazar las listas negras. Del mismo modo, a medida que empezaron a llegar más dispositivos a las redes corporativas, se desarrollaron varios sistemas de control de acceso para autenticar, tanto los dispositivos como los usuarios que se sientan detrás de ellos, y para autorizar a los usuarios y dispositivos para acciones específicas.



Más recientemente, las preocupaciones sobre la autenticidad del software y la protección de la propiedad intelectual dieron lugar a diversas técnicas de verificación de software y de certificación. Por último, la confidencialidad de los datos siempre ha sido y sigue siendo una preocupación primordial. Los controles como redes privadas virtuales (VPN) o la encriptación de medios físicos, como 802.11i (WPA2) o 802.1AE (MACsec), se han desarrollado para garantizar la seguridad de los datos.

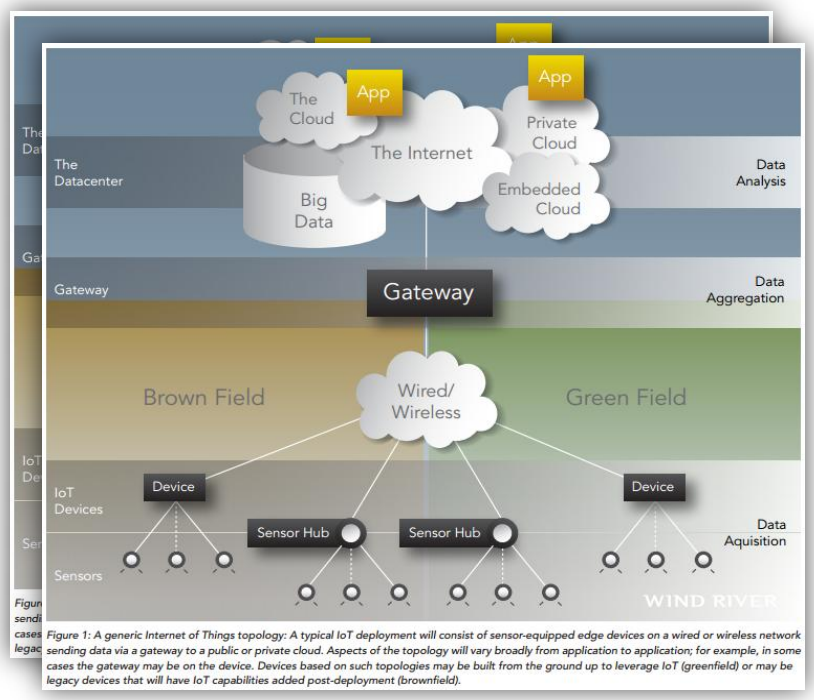


Figure 1: A generic Internet of Things topology: A typical IoT deployment will consist of sensor-equipped edge devices on a wired or wireless network sending data via a gateway to a public or private cloud. Aspects of the topology will vary broadly from application to application; for example, in some cases the gateway may be on the device. Devices based on such topologies may be built from the ground up to leverage IoT (greenfield) or may be legacy devices that will have IoT capabilities added post-deployment (brownfield).

Las nuevas amenazas, restricciones y desafíos

La aplicación de estas mismas prácticas o variantes en el mundo del Internet de las Cosas requiere una reingeniería sustancial para hacer frente a las limitaciones de los dispositivos. Las listas negras, por ejemplo, requieren demasiado espacio en disco para ser prácticas para las aplicaciones del IoT. Los dispositivos incrustados están diseñados para un bajo consumo de energía, con un pequeño factor en forma de silicio y, a menudo, poseen una conectividad limitada. Por lo general solo tienen la capacidad de procesamiento y memoria necesarios para realizar sus tareas. Y son a menudo “sin cabeza”, es decir, no hay un ser humano que opere con ellos, que pueda introducir credenciales de autenticación de entrada o decidir si una aplicación debería ser de confianza; ellos tienen que hacer sus propios juicios y tomar decisiones sobre si se debe aceptar un comando o ejecutar una tarea.

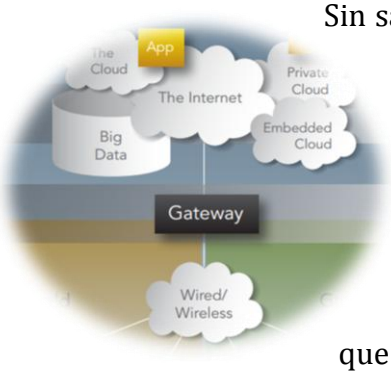
La infinita variedad de aplicaciones del IoT plantea igualmente una amplia variedad de desafíos de seguridad. Por ejemplo:

- En la automatización de la planta de una fábrica están profundamente incrustados los controladores lógicos programables (PLC), que operan sistemas robóticos que están normalmente integrados con la infraestructura de las TIs de la empresa. ¿Cómo pueden los PLCs estar protegidos de toda interferencia humana y, al mismo tiempo, proteger la inversión en la infraestructura de las TIs y el aprovechamiento de los controles de seguridad disponibles?

- Del mismo modo se unen a la infraestructura los sistemas de control para reactores nucleares. ¿Cómo pueden recibir actualizaciones de software o parches de seguridad de manera oportuna y sin menoscabo de la seguridad funcional o incurrir en costes significativos de recertificación cada vez que un parche es lanzado al mercado?

- Un medidor inteligente capaz de enviar datos de uso de energía al operador de la red para la facturación dinámica o para la optimización de energía en tiempo real debe ser capaz de proteger esa información del uso o de la divulgación no autorizada.

Construir seguridad a partir de sus cimientos



Sin saber si un solo mando de control va a proteger adecuadamente un dispositivo, ¿cómo podemos aplicar lo que hemos aprendido en los últimos 25 años para implementar la seguridad en una variedad de escenarios? Lo hacemos a través de un enfoque de múltiples capas de seguridad que comienza al principio, cuando se aplica energía. Se establece una base informática de confianza y anclas que confían en algo inmutable que no puede ser manipulado.

La seguridad debe ser abordada a lo largo del ciclo de vida del dispositivo, desde el diseño inicial hasta el entorno operativo:

1. ***Arranque seguro:*** Cuando la conexión es introducida por primera vez al dispositivo, la autenticidad y la integridad del software en el dispositivo se verifica mediante el uso de firmas digitales generadas criptográficamente. De la misma manera que una persona firma un cheque o un documento legal, una firma digital adjunta a la imagen de software y verificada por el dispositivo asegura que solo el software que ha sido autorizado para funcionar en ese dispositivo, y firmado por la entidad que lo autorizado, serán cargados. La base de la confianza se ha establecido, pero el dispositivo aún necesita la protección de diversas amenazas e intenciones maliciosas en tiempo de ejecución.

2. ***Control de acceso:*** A continuación se aplican diferentes formas de recursos y control de acceso. Los controles de acceso obligatorios o basados en funciones incorporadas en el sistema operativo limitan los privilegios de los componentes del dispositivo y las aplicaciones para el acceso solo a los recursos que necesitan para hacer su trabajo. Si cualquiera de los componentes se ve comprometido, el control de acceso asegura que el intruso tenga acceso como mínimo a otras partes del sistema como sea posible. Los mecanismos de control de acceso en los dispositivos son análogos a los sistemas de control de acceso en la red, tales como Microsoft Active Directory: incluso si alguien se las arregla para robar credenciales corporativas para obtener acceso a una red, la información comprometida estaría limitado a solo aquellas áreas de la red autorizadas por dichas credenciales particulares. El principio de privilegios mínimos dicta que solo el acceso mínimo requerido para realizar una función debería ser autorizado con el fin de minimizar la efectividad de cualquier violación de la seguridad.

3. ***Autenticación de dispositivos:*** Cuando el dispositivo está conectado a la red, debe autenticarse antes de recibir o transmitir datos. Los dispositivos profundamente arraigados no tienen a menudo a los usuarios sentados detrás de los teclados a la espera de dar entrada a las credenciales necesarias para acceder a la red. ¿Cómo, entonces, podemos asegurarnos de que los dispositivos estén correctamente identificados antes de la autorización? Así como la autenticación de usuario le permite acceder a una red corporativa basada en nombre de usuario y contraseña, la autenticación de máquina permite a un dispositivo acceder a una red basada en un conjunto similar de credenciales almacenadas en un área de almacenamiento seguro.

4. ***Cortafuegos e IPS:*** El dispositivo también tiene un firewall o capacidad de inspección profunda de paquetes para controlar el tráfico que está destinado a acabar en el dispositivo. ¿Por qué es necesario el firewall o IPS si los aparatos basados en la red están en su lugar? Los dispositivos profundamente arraigados tienen protocolos únicos, distintos de los protocolos de la TI de la empresa. Por ejemplo, la red de energía inteligente tiene su propio conjunto de protocolos que rigen cómo los dispositivos se comunican entre sí. Por eso se necesitan protocolos específicos de filtrado y capacidades de inspección profunda de paquetes para identificar cargas maliciosas escondidas en los protocolos que no son de la TI. El dispositivo no necesita preocuparse por el filtrado a nivel superior, pero es necesario para filtrar los datos específicos destinados a terminar en ese dispositivo de manera que haga un uso óptimo de los limitados recursos computacionales disponibles.

5. ***Actualizaciones y parches:*** una vez que el dispositivo esté en funcionamiento, se iniciará la recepción de parches y actualizaciones de software. Los operadores tienen que desplegar parches y los dispositivos necesitan autenticarlos, de manera que no consuman ancho de banda o dañen la seguridad de funcionamiento del dispositivo. Es como cuando Microsoft envía actualizaciones para los usuarios de Windows y "ata" sus ordenadores portátiles durante 15 minutos. Otra cosa muy distinta es cuando miles de dispositivos están desempeñando funciones o servicios críticos y dependen de los parches de seguridad para protegerse contra la inevitable vulnerabilidad que escapa a la naturaleza. Las actualizaciones de software y parches de seguridad deben ser entregados de manera que se conserve el limitado ancho de banda y la conectividad intermitente de un dispositivo embebido y se elimine totalmente la posibilidad de poner en peligro la seguridad funcional.

Comienza en el Sistema Operativo (SO)

La seguridad no puede ser pensada como complemento a un dispositivo, sino más bien como parte integral de un funcionamiento fiable del mismo. Los controles de seguridad del software necesitan ser introducidos a nivel del sistema operativo, aprovechando las capacidades de seguridad de hardware que ahora entra en el mercado, y se extienden a través de los dispositivos para mantener continuamente una base informática de confianza. La construcción de la seguridad a nivel del sistema operativo toma la responsabilidad de los diseñadores de dispositivos y desarrolladores para configurar sistemas que mitiguen las amenazas y garanticen que sus plataformas son seguras.

A menudo, la única diferencia entre las consideraciones de seguridad y protección es la intención que hay detrás de ellas.

La solución de seguridad de extremo a extremo

La seguridad, tanto a nivel de dispositivo como de red, es fundamental para el funcionamiento del IoT. La misma inteligencia que autoriza a los dispositivos a realizar sus tareas también debe permitirles reconocer y contrarrestar las amenazas. Afortunadamente, esto no requiere un enfoque revolucionario, sino más bien una evolución de las medidas que han tenido éxito en las redes de la TI, adaptado a los retos del IoT y las limitaciones de los dispositivos conectados. En lugar de buscar una solución que aún no existe, o proponer un enfoque revolucionario para la seguridad, Wind River se centra en la entrega de los controles actuales de seguridad de la TI con tecnología de última generación, optimizada para las nuevas y extremadamente complejas aplicaciones integradas que impulsan el Internet de las Cosas.