Seguridad, gran reto para internet de las cosas

El desarrollo de procesos automatizados para verificar software es uno de los pasos que se están dando para avanzar en la tecnología que facilitará la comunicación de diferentes aparatos a través de la red. Colombia va rezagada del mundo porque falta conectividad e inversión.

En un sistema eléctrico con elementos distribuidos, un control central toma las decisiones con base en los informes de consumo de cada una de las terminales de los usuarios. Estas redes han sido un punto de partida para el diseño del internet de las cosas.

Foto: Instant Vantage, creative commons

Sandra Rueda, profesora del Departamento de Ingeniería de Sistemas y Computación (DISC, Uniandes), explica qué es el internet de las cosas (IoT, por sus siglas en inglés), por qué la seguridad aún falla en la red y, por lo tanto, hace que sea todavía vulnerable.

¿Cómo describe el internet de las cosas?

Es una red de dispositivos inteligentes interconectados. Estos dispositivos cuentan con una cierta autonomía y además pueden responder a comandos remotos enviados por sus propietarios, vía internet. Esos comandos iniciarían la ejecución de una acción, como encender o apagar un horno o una alarma en una casa permitiendo, entre otras ventajas, ahorrar energía. Los dispositivos inteligentes "toman decisiones" de forma autónoma con base, por ejemplo, en lecturas que obtienen de sensores. Hay otros escenarios donde la toma de decisiones depende de información recopilada a partir de elementos distribuidos, como en el caso *smart grid,* donde un control central decide cómo distribuir electricidad, con base en el reporte de consumo que dan los medidores de las casas. El contexto internet de las cosas se parece al contexto de *smart grid* y busca mejorar la toma de decisiones.

¿Qué retos se enfrentan con el internet de las cosas?

En seguridad, un problema es garantizar que los comandos emitidos de manera remota para que los dispositivos ejecuten una orden, provengan de la persona autorizada para darlos. Otra de las preocupaciones es la privacidad de las personas.

¿Esto implicaría un control central?

No necesariamente. Pero, por ejemplo, si alguien tiene una cámara de video en línea para vigilar que una niñera haga su trabajo, y la conexión no está protegida, cualquiera podría saber lo que sucede en esa casa.

¿Los protocolos de seguridad y los mecanismos para controlar todas esas vulnerabilidades avanzan rápido?

Eso está mejorando, pero se diseña un paso atrás de lo que pretende proteger. Internet se desarrolló de una forma y se usó

de otra. A nadie se le ocurrió que el requerimiento de seguridad iba a ser crítico y los problemas se trataron de resolver con parches. Ahora los diseñadores y desarrolladores, tanto de programas y aplicaciones como de dispositivos electrónicos, son más conscientes de la situación y el problema de seguridad se está empezando a abordar de manera integral en todos los componentes. Pero todavía aparecen aplicaciones con vulneabilidades y aparatos cuyo protocolo de comunicación es seguro, pero el usuario no entiende, por ejemplo, que hay cierta información que no debe revelar o programas que no debe instalar porque puede olvidar algo, pues la actividad es manual.

Además es posible que los desarrolladores introduzcan, sin intención, errores en el código de una aplicación o en sus protocolos, y aún no contamos con tecnología adecuada para evaluar de manera automatizada estos procesos. En este escenario, las acciones son muy limitadas, a pesar de que hay listas de chequeo, algunas herramientas de evaluación y pruebas exhaustivas de software. El problema es que un desarrollador puede olvidar algo. Este olvido puede ocurrir cuando la actividad es manual.

Sandra Rueda, profesora asistente del Departamento de Ingeniería de Sistemas y Computación.

> “Estos aparatos, como las ciudades inteligentes, están empezando a almacenar mucha información de los usuarios: a qué horas llega, a qué hora se va, qué elementos usa. Así que una de las preocupaciones es la privacidad de las personas”.

Para resolver este tipo de problemas se trabaja en técnicas de evaluación automática para que, en lo posible, se detecten los problemas y se puedan corregir a tiempo. También se están mejorando las técnicas de detección dinámica para incorporar mecanismos de reacción a sucesos desconocidos. ■

Cuando las máquinas **deciden**

La Facultad de Ingeniería de Los Andes organizó la Conferencia Colombiana de Comunicaciones y Computación (Colcom) en junio pasado, sobre el internet de las cosas (IoT por sus siglas en inglés) como habilitador de nuevos mercados de las TIC. El evento es el más importante del capítulo colombiano de la IEEE (Institute of Electrical and Electronics Engineers) y se realiza para mostrar “los avances y el desarrollo del uso académico, científico e industrial de las diferentes áreas de las telecomunicaciones y la informática”.

Dispositivos colocados en el interior del cuerpo que detectan las necesidades del organismo y suministran los medicamentos al enfermo; automóviles que se comunican entre sí para informar de hechos fortuitos y evitar accidentes; nanorrobots que determinan los cambios en las condiciones de los ríos y alertan a las autoridades para tomar decisiones sobre suministro de agua a una población. Estas y, al parecer, cualquiera de las opciones que se le ocurran a la imaginación, son las posibilidades que se avecinan con el internet de las cosas, IoT.

La evolución natural de la web condujo hasta el IoT, un fenómeno que cambiará radicalmente la vida cotidiana de las personas. Sus antecedentes pueden encontrarse en la *smart grid*, diseñada para mejorar el esquema de distribución eléctrica, y en los conceptos de *smart buldings* y *smart cities*, que han posibilitado el estado actual de esta tecnología.

Sin embargo, los ingenieros deben trabajar en maximizar la seguridad y en minimizar el consumo de energía para evitar los