

La clasificación de dispositivos del Internet de las Cosas basada en sus impactos en los seres vivos

Felix Uribe
felix@uribe100.com
Uribe100.com

Introducción

Este ensayo describe cómo clasificar dispositivos que pertenecen al Internet de las Cosas o IoT¹ basado en sus impactos en los seres vivos. La clasificación de IoT que propongo se basa en el impacto potencial (físico, económico o social) a los seres vivos en el caso de que la confidencialidad, disponibilidad o integridad de la información, las operaciones internas o los componentes del dispositivo de IoT se vean comprometidas. A medida que millones y millones de dispositivos IoT se construyen y se introducen en el ecosistema del mundo, la capacidad de poder clasificar sus impactos en humanos, animales y plantas nos permitirá identificar y abordar muchas de las cuestiones de seguridad y privacidad que afectan actualmente la confiabilidad de estos dispositivos.

Descripción

Aunque no hay una definición estándar para el IoT, me referiré a ella como la red de dispositivos (cosas) capaces de interactuar con otros dispositivos y seres vivos a través del Internet o a través de una red privada local o global no conectada al Internet.

Las recientes proyecciones de crecimiento de estos dispositivos sugieren que para el año 2020 el número de dispositivos conectados en el planeta alcanzará aproximadamente cincuenta mil millones (Cisco, 2011). Además de este crecimiento, se espera que el número de dispositivos de IoT comprometidos por cibercriminales se intensifique (Stroz Friedberg, 2017). Está claro que dentro de unos años y debido al rápido crecimiento de la tecnología, los dispositivos IoT se convertirán en una parte omnipresente de nuestras vidas y ecosistemas. Por lo tanto, se debe desarrollar un mejor método de clasificación.

Metodología de Clasificación

Los dispositivos IoT pueden clasificarse de muchas maneras. Por ejemplo, pueden clasificarse en función del tipo de datos que manejan, como médicos, financieros o del sector en nuestra sociedad

¹ Internet of Things (IoT) por sus siglas en inglés. Las siglas IoT serán utilizadas para referirnos al Internet de las Cosas a través del documento.

donde se utilizan, tales como la manufactura, el transporte, el comercio minorista, el consumidor y el hogar.

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos categoriza los sistemas de información y su información basados en «el impacto potencial en una organización en caso de que ocurran ciertos eventos que ponen en peligro los sistemas de información e información que necesita la organización para cumplir con su misión asignada, proteger sus activos, sus responsabilidades legales, mantener sus funciones cotidianas y proteger a las personas» (NIST, 2004). De manera similar, la clasificación de IoT que propongo para dispositivos IoT se basa en el impacto potencial en los seres vivos² en el caso de que la confidencialidad, disponibilidad o integridad de la información³, las operaciones internas o los componentes⁴ del dispositivo se vean comprometidas.

La confidencialidad, integridad y disponibilidad constituyen los «objetivos de seguridad». La «pérdida» de cada uno de estos objetivos se definen a continuación:

Confidencialidad: Preservar la divulgación no autorizada de la información, las operaciones internas y los componentes del dispositivo IoT.

Pérdida: Divulgación no autorizada de la información del dispositivo IoT, operaciones internas o componentes.

Integridad: Mantener la integridad (veracidad) de la información del dispositivo IoT, las operaciones internas y los componentes.

Pérdida: Modificación o destrucción de la información del dispositivo IoT, operaciones internas o componentes.

Disponibilidad: Acceso ininterrumpido a la información del dispositivo IoT, operaciones internas y componentes.

Pérdida: No se puede acceder a la información del dispositivo, operaciones internas o componentes.

² Humanos, animales y plantas.

³ La información puede ser datos de sensores, información personal, sistema operativo, aplicaciones de software o cualquier otro tipo de datos recopilados, almacenados, procesados y compartidos por el dispositivo IoT.

⁴ Los componentes de un dispositivo IoT pueden ser microcontroladores, sensores, actuadores, memoria, almacenamiento y otros componentes que están incrustados o conectados al dispositivo y que forma parte de su funcionamiento.

Basándose en estas definiciones, un dispositivo IoT puede clasificarse como uno de estos tipos.

Tipo A	Si la pérdida de uno o de todos los objetivos de seguridad causa graves daños físicos, económicos o sociales al ser vivo ⁵ . Por ejemplo, un mal funcionamiento de un marcapasos inalámbrico, un sistema de frenos de un automóvil o un sistema de riego agrícola.
Tipo B	Si la pérdida de uno o de todos los objetivos de seguridad causa un daño físico, económico o social menor al ser vivo ⁶ . Por ejemplo, un mal funcionamiento de uno de los componentes de un sistema de climatización puede causar agotamiento por calor a los seres humanos y animales.
Tipo C	Si la pérdida de uno o todos los objetivos de seguridad causa muy poco o ningún daño al ser vivo. Por ejemplo, una caja registradora no puede procesar transacciones financieras en línea.

La selección de cualquier tipo de IoT por un individuo u organización es una decisión basada en el riesgo y que puede tomar en cuenta otros factores exclusivos de sus funciones personales u organizacionales. Un dispositivo IoT puede clasificarse como un tipo A en una organización, mientras que otra organización puede clasificarla como un tipo B, aunque sea el mismo dispositivo. Además, las personas u organizaciones pueden expandir cada tipo con «subtipos» para ofrecer una sub-clasificación o crear un índice de riesgo de IoT. Por ejemplo, Tipo A (1) = sistema de soporte de vida, Tipo A (2) monitor de presión arterial inalámbrico independiente.

Ejemplos de dispositivos IoT y sus tipos.

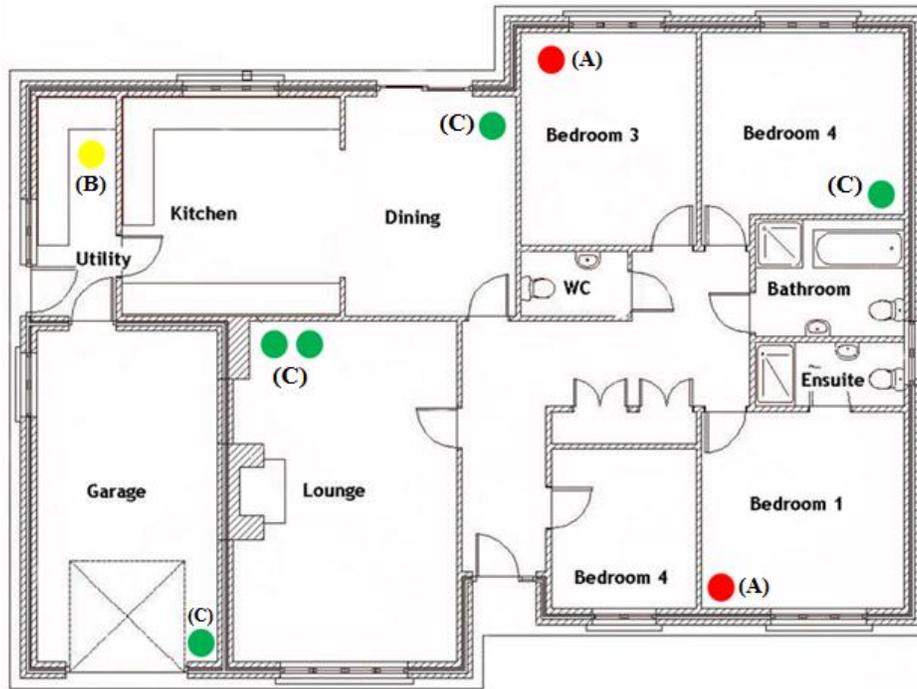
(Código de color, Tipo A (rojo), Tipo B (amarillo) y Tipo C (verde))

Tipo A	Tipo B	Tipo C
Equipos de monitoreo médicos, implantes inalámbrico, automóviles inteligentes.	Sistemas de climatización, semáforos.	Alarmas, lavavajillas, cámaras, luces, abridor de garaje.

⁵ Ejemplos de graves daños físicos, económicos o sociales pueden incluir lesiones graves, muerte, robo de identidad y pérdida de reputación.

⁶ Ejemplos de daños físicos, económicos o sociales menores pueden incluir incapacitación temporal y daño del crédito financiero personal.

El siguiente plano muestra la ubicación y el tipo de los dispositivos IoT en un hogar inteligente.



Basándose en esta información, es fácil de ver que los dormitorios 1 y 3 contienen un dispositivo IoT de tipo A y el cuarto de servicio uno de tipo B.

Una vez conocidos los tipos de dispositivos IoT, se puede realizar una evaluación de seguridad y privacidad en una infraestructura IoT y se pueden implementar los controles, políticas y procedimientos de seguridad y privacidad necesarios para cada tipo de dispositivo o grupo de dispositivos.

Conclusión

El crecimiento exponencial de los dispositivos IoT y sus aplicaciones cotidianas exige su clasificación para abordar las preocupaciones actuales de seguridad y privacidad que afectan la confiabilidad del actual dominio de IoT en el mundo. Ésta clasificación ofrece a los usuarios actuales de estos dispositivos la capacidad de ver y comprender los riesgos y encontrar una manera efectiva de implementar controles de seguridad y privacidad entornos a estos. Los fabricantes de dispositivos de IoT deben tener en cuenta esta clasificación durante el diseño y la fabricación de los mismos para garantizar que la seguridad y la privacidad se implementen por diseño y no aparezcan como una idea posterior durante el ciclo de vida de estos dispositivos.

Referencias

Evans D. (2011). *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*. Disponible en:

http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

NIST (2004). *Standards for Security Categorization of Federal Information and Information Systems*. Disponible en: <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>

Stroz Friedberg (2017). *2017 Cybersecurity Predictions*. Disponible en:

[https://www.strozfriedberg.com/wp-content/uploads/2017/01/2017-Stroz-Friedberg-Cybersecurity-Predictions-](https://www.strozfriedberg.com/wp-content/uploads/2017/01/2017-Stroz-Friedberg-Cybersecurity-Predictions-Report.pdf?utm_campaign=CYBER%202017%20PREDICTIONS%20CAMPAIGN&utm_source=IoT%20Blog%20Postm)

[Report.pdf?utm_campaign=CYBER%202017%20PREDICTIONS%20CAMPAIGN&utm_source=IoT%20Blog%20Postm](https://www.strozfriedberg.com/wp-content/uploads/2017/01/2017-Stroz-Friedberg-Cybersecurity-Predictions-Report.pdf?utm_campaign=CYBER%202017%20PREDICTIONS%20CAMPAIGN&utm_source=IoT%20Blog%20Postm)