Contacto

Ciberseguridad para IoT

Ciberseguridad IoT a todos los niveles

Un sistema IoT está compuesto de diversos dispositivos conectados – compuestos a su vez por diferentes componentes integrados – y una infraestructura de gestión, control y procesado.

Applus+ Laboratories dispone de un equipo de ingenieros con experiencia en evaluaciones de seguridad hardware, software y protocolos de comunicación preparados para evaluar la ciberseguridad de componentes IoT, dispositivos IoT así como del sistema IoT en su conjunto.

- Evaluaciones de ciberseguridad de componentes IoT
- Evaluaciones de ciberseguridad de dispostivos IoT

- Evaluaciones de ciberseguridad de sistemas IoT

Evaluación de componentes IoT

Cada dispositivo IoT está formado por múltiples componentes siendo estos en donde se delegan las principales funcionalidades de seguridad. De ahí la importancia de integrar componentes certificados o que su seguridad haya sido evaluada.

Evaluaciones de seguridad bajo un esquema de certificación:
Applus+ es un laboratorio de seguridad acreditado para evaluar componentes hardware y software embebidos en los dispositivos IoT bajo diversos esquemas de certificación de reconocimiento internacional:

- Common Criteria (SOG-IS Lab)
- PSA Certified (Accredited Lab)
- Fido (Authentication solutions)
- GlobalPlatform (TEE - Trusted Execution Environments)

Evaluaciones independientes a medida*:
En aquellos casos en los que no es necesario que el componente esté certificado pero el fabricante requiera que la seguridad de su producto esté evaluada, Applus+ ofrece un servicio de evaluaciones independientes y a medida para cada tipo de componente y caso de uso. Estas evaluaciones se adaptan a las necesidades del cliente: white/grey /black box, source code review, vulnerability analysis, design review, etc.

Evaluación de dispositivos IoT

Evaluación bajo esquemas de certificación:
Applus+ puede realizar evaluación de seguridad de soluciones IoT bajo el esquema Common Criteria. Asimismo, se están desarrollando otros

esquemas de certificación para
IoT en los que la evaluación
podría basarse. Consúltanos para más información sobre estas nuevas certificaciones.

Evaluaciones independientes de ciberseguridad*:
Conscientes de la gran variedad de casos de uso dentro del ámbito de IoT, nuestros expertos adaptan la evaluación a las particularidades del producto teniendo en cuenta su naturaleza, el tipo de solución IoT de la que formará parte o el tipo de datos que gestionará. No tiene la misma criticidad una bombilla inteligente, el gateway que gestiona la iluminación de un hotel o el smart meter de la compañía eléctrica). Nuestras evaluaciones analizan los siguientes aspectos, aunque nos adaptamos a las necesidades del cliente:

- **Protección de datos:** Los dispositivos IoT pueden almacenar y comunican información sensible como claves criptográficas o datos personales que deben ser protegidos. Por ello evaluamos la seguridad de las comunicaciones para todo tipo de protocolos (BLE, Zigbee, Wi-Fi, LTE, etc.), así como la seguridad de los mecanismos de almacenamiento (protección de activos)
- **Seguridad de los interfaces:** Todos los interfaces de acceso al dispositivo IoT deben identificarse, evaluar su grado de protección, así como los mecanismos de autentificación/identificación: Interfaces web, interfaces de red (puertos abiertos inseguros), interfaces físicos (JTAG, UART, etc.), API Cloud o API Mobile.
- **Actualizaciones seguras:** ¿Cuál es el mecanismo para realizar las actualizaciones de forma segura? ¿Hay algún protocolo para validar la integridad y autenticidad del nuevo binario? Nuestros expertos evalúan los sistemas de actualización y los protocolos de patching.
- **Arranque seguro:** ¿Cuál es el mecanismo del sistema de arranque / reinicio (boot) del dispositivo? Realizamos una evaluación del protocolo de arranque del equipo para asegurar que son seguros y de confianza.

Metodologías y guías de buenas prácticas: A día de hoy la mayoría de países están todavía desarrollando su propia regulación/estándares IoT, pero existen metodologías y guías de buenas prácticas en las que se puede basar la evaluación, como:

- GSMA IoT Security Guidelines and Assessment
- OWASP IoT Top 10
- Code of Practice for consumer IoT security
- ENISA Baseline Security Recommendations for IoT.

Consúltanos si estás interesado en una evaluación conforme a estas metodologías/guías.

Evaluación de sistemas IoT

La seguridad de un sistema IoT va más allá de la protección de cada uno de sus dispositivos. Aunque estos puedan ser seguros de forma aislada, una vez de despliegan y conectan pueden aparecer nuevas amenazas en el sistema. Del mismo modo, la gestión de la cadena de suministro es un aspecto crucial ya que la seguridad de nuestro sistema depende en gran medida de la confianza en todos los elementos que lo componen.

Análisis de seguridad de la cadena de suministro:
Un solo dispositivo vulnerable puede comprometer todo el sistema. Debemos conocer los dispositivos y soluciones que conforman nuestro sistema, para ello tenemos que contar una cadena de suministro de confianza. ¿Cómo puede Applus+ ayudarte a lograrlo?

- Evaluaciones de riesgos y amenazas en la cadena de suministro

- Auditorias de seguridad de los planes de desarrollo y fabricación
- Ensayos de seguridad de las soluciones que no dispongan de un certificado de seguridad reconocido
- Evaluación de riesgos y amenazas del sistema
- Evaluación de las diferentes capas (cloud, fog, remote mobile controllers) y sus interfaces.

*Nota: Dado que Applus+ Laboratories está acreditado como laboratorio independiente por varios esquemas de certificación, los ingenieros de Applus+ nunca participan en el desarrollo de producto o la implementación de soluciones, garantizando así su imparcialidad. Nuestra evaluaciones independientes no están acreditadas y su objetivo es que el desarrollador disponga de información y de unos resultados de la evaluación para entener el nivel de seguridad de sus productos a pesar de que no exista todavía un esquema de certificación aplicable.