Implementación segura de sistemas de IoT

Osvaldo Marianetti, Ernesto Chediak y Daniel Fontana

[1]Universidad de Mendoza. Facultad de Ingeniería. Mendoza. Argentina
osvaldo.marianeti@um.edu.ar, ernesto.chediack@um.edu.ar,
daniel.fontana@um.edu.ar

Abstract. Cuando se hace referencia a una seguridad inteligente para sistemas computacionales, reducir la superficie de ataque es fundamental. De hecho, garantizar que la superficie de ataque sea lo más pequeña posible es una medida de seguridad básica.
La superficie de ataque de una organización es la suma de vulnerabilidades, vías o métodos (a veces llamados vectores de ataque) que los intrusos pueden utilizar para obtener acceso no autorizado a la red o a datos confidenciales, o bien para perpetuar un ciberataque. Los expertos en seguridad dividen la superficie de ataque en tres subsuperficies: la superficie de ataque digital, la superficie de ataque física y la superficie de ataque de ingeniería social.
La superficie de ataque física expone activos e información generalmente accesible solo a usuarios con acceso autorizado a dispositivos de punto final o de oficina físicos de una organización (servidores, computadoras, dispositivos móviles, dispositivos de IoT, hardware operativo).
Este trabajo propone, a partir del paradigma de Computación en la Niebla, que los dispositivos lógicos programables como las FPGA, con capacidades de reconfiguración y gran potencia computacional, son una alternativa de desarrollo para la reducción de la superficie de ataques que presenta la implementación segura de sistemas de IoT.

Keywords: Seguridad, Computación en la niebla, IoT.

1 Introducción

En la introducción de este trabajo se propone demostrar que, a partir del paradigma de Computación en la Niebla y las caracterpisticas de los dispositivos lógicos programables como las FPGA (Field Programmable Logic Array), estos componentes se pueden considerar una alternativa de desarrollo frente a las problemáticas involucradas en la implementación segura de sistemas de IoT e IoE, teniendo en cuenta las vulnerabilidades que se presentan en las distintas capas de estos sistemas y en la reducción de la superficie de ataque.

Algunas de las principals causas que hacen a un sistema de IoT vulnerable son:
a) La heterogeneidad de tecnologías. Son necesarios conversiones de protocolos y hacer compatibles los mecanismos de seguridad implementados por distintos fabricantes.

b) Los dispositivos IoT no cuentan en la actualidad con la capacidad de computación que requieren las medidas de seguridad que se adoptan en otras plataformas.
c) Las comunicaciones de toda la tecnología IoT se soporta casi totalmente en el aire, es decir comunicaciones inalámbricas. Esta es la tecnología que más tipos de ataque puede sufrir, cuando precisamente el intercambio de información de los dispositivos IoT son bastante predecibles y su arquitectura y formato no son fáciles de cambiar.

En el caso particular de las redes de sensores inalámbricos (WSN) están constituidas por grupos de nodos de dispositivos embebidos con conexión inalámbrica (sensores, microcontrolador o procesador más un módulo transmisor/receptor). Uno de los principales problemas a resolver en las WSN es optimizar los recursos de procesamiento, ya que las WSN utilizan en su despliegue nodos con procesadores o microcontroladores de propósito general. Para esta problemática se ha propuesto que los nodos cuenten con procesadores de "soft-core" (arquitectura configurable). Esto optimiza la arquitectura del procesador para que se pueda adaptar a las necesidades de las aplicaciones de las redes de sensores. [1]

2 Computación en el borde y computación en en la niebla.

El escenario tecnológico definido por Internet de las Cosas y por aplicaciones que demandan respuesta en tiempo real, plantea a los desarrolladores en el campo de las tecnologías de la información y las comunicaciones, desafíos de carácter funcional y tecnológico. La computación en la niebla y la computación en el borde constituyen una alternativa para hacer frente a algunos de esos desafíos como la movilidad, la respuesta en tiempo real y el uso eficiente de recursos.

La computación en el borde ofrece un mejor procesamiento de los datos para las aplicaciones basadas en la nube, el cual realiza más cerca de la fuente de los mismos, en el borde de la red. Gracias a esta característica se alcanzan beneficios como menor latencia entre la aplicación cliente y el servicio en la nube; acercamiento del usuario y los dispositivos a los contenidos con un uso más eficiente de los recursos de red.

Por su parte, la computación en la niebla enfatiza el procesamiento en la infraestructura local de red, más que en los dispositivos y extiende los recursos de computación hacia el borde de la red, en un modelo distribuido. Así, se dispone en el borde de los servicios de procesamiento, almacenamiento y monitoreo provistos por el enfoque tradicional en la nube, por medio de instancias denominadas "fog nodes". Estos nodos realizan un procesamiento previo de los datos a la nube, en los dispositivos IoT ubicados en el borde, con beneficios potenciales como menor latencia entre los dispositivos de usuario final y los nodos en la niebla; soporte a requerimientos de movilidad; habilitación de la ubicuidad de los servicios de computación y viabilidad de interacciones en tiempo real.

3 Tecnología de lógica reconfigurable.

La tecnología de lógica reconfigurable es un prestador de soluciones eficientes, escalables y sostenibles para estos escenarios, donde el creciente número de sensores que se

implementan en hogares inteligentes, fábricas inteligentes y ciudades inteligentes plantea a los desarrolladores un abordaje acorde a estos sistemas. Por un lado, las nuevas aplicaciones de IoT requieren una conectividad mejorada para comunicarse de manera eficiente a través de una amplia gama de interfaces y protocolos nuevos y heredados. Por otro lado, a medida que los usuarios requieran mayores niveles de inteligencia, los diseñadores necesitarán más recursos computacionales para el procesamiento en tiempo real de los datos cercanos a los sensores. En un número cada vez mayor de aplicaciones, se hace necesario una solución programable que combine E/S flexibles, una arquitectura configurable, operación de energía baja en un factor de forma pequeño y precio para producción de alto volumen.

Los fabricantes de FPGAs ofrecen chips con funciones adecuadas para abordar estas necesidades. Están diseñados específicamente para desarrollarar soluciones energéticamente eficientes que satisfagan las demandas de procesamiento de los productos industriales y de Internet de las cosas (IoT). A pesar de agregar una amplia funcionalidad, algunos de ellos solo consumen 75 µA de corriente estática. Por ejemplo, el iCE40 UltraPlus FPGA de Lattice Semiconductor disponible en densidades de 2800 o 5280 LUT, cuenta con 80 Kb o 120 Kb de RAM de bloque, cuatro u ocho bloques DSP de 16 x 16 multiplicados o acumulados de 16 bits para el procesamiento de señales y 1 Mb de RAM en cuatro puertos individuales de 256 Kb bloques de memoria. [2]

En el caso de cifrado de datos de sensores, las capacidades integradas de las FPGA, en particular su arquitectura paralela y su capacidad para interactuar con una amplia gama de sensores, también se puede utilizar para crear dispositivos IoT en el borde más seguros. Para abordar esta creciente necesidad, se han desarrollado modelos que implementan un bloque de criptografía para proteger los datos destinados a dispositivos IoT. Implementado en una FPGA, el bloque utiliza encriptación 128, toma datos de un sensor, los cifra mediante el cifrado AES 128 y los envía, genera claves privadas y públicas y las almacena en una memoria segura. Como resultado, los datos capturados por la FPGA de los sensores se pueden transferir de forma segura a un servidor o a la nube.[3]

4 Arquitectura de sistema embebido basada en soft_processors

Se presenta en esta sección el diseño de una arquitectura de un sistema embebido basada en soft_processors. Esta arquitectura tiene la misma funcionalidad de los sistemas comerciales incluyendo componentes de seguridad en su diseño, pero incorpora las características de la naturaleza del hardware reconfigurable, para que el sistema sea más resistente a ataques. En la arquitectura basada en FPGA sus unidades funcionales (memorias, puertos, controladores, temporizadores, etc.) son reconfigurables y adaptables a nuevos requerimientos, incluso en forma remota. La fig. 1 representa la arquitectura basada en FPGA.

Para el desarrollo de la arquitectura del sistema embebido basada en soft_processors, se ha utilizado el entorno de desarrollo Quartus II (versiones 13.1 web edition y Quartus Prime Lite Edition 17.0) La herramienta QSYS de estos entornos para le generación del SOPC (sistema programable en el chip) y el entorno NIOS II software build tool for Eclipse para la programación del soft_processor NIOS II/e. Como procesador de

comunicaciones se ha utilizado un módulo ESP 8266. El ESP8266 soporta el protocolo SPI por hardware. En la implementación de este trabajo se utiliza un bloque SPI instanciado en la FPGA como elemento Maestro, el cual se comunica con el procesador NIOS II y el módulo ESP 8266 como esclavo que recibe y envía datos mediante protocolo WIFI. Este componente es el único externo al sistema programable en el chip (SOPC). En cuanto al circuito del módulo de seguridad se ha utilizado la implementación de un algoritmo AES de 128 bits.

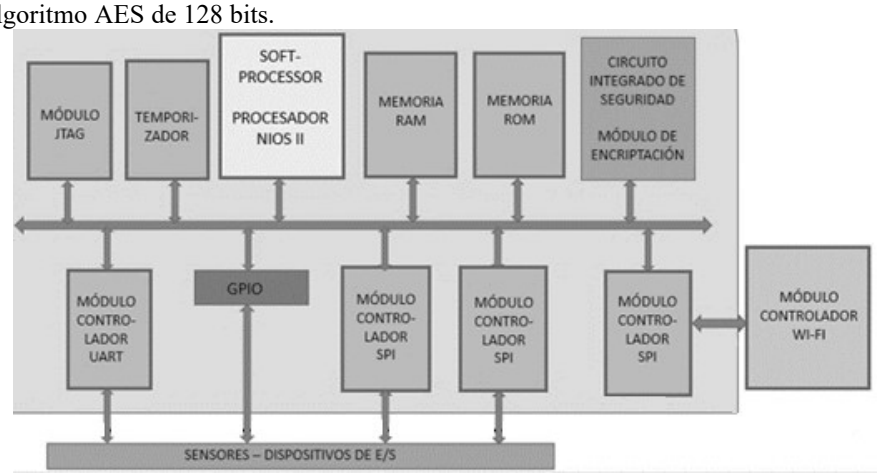

Fig. 1. La figura representa la arquitectura de un sistema embebido basada en soft_processors donde se presentan todos los compnentes instanciados en una FPGA.

5 Conclusión

Este ejemplo constituye un modelo que permite avanzar en el desarrollo de arquitecturas de sistemas programables en un chip (SOPC) con dispositivos reconfigurables, optimizados para operar como nodo de una WSN y también en aplicaciones de sistemas de IoT que pueda actuar como concentradores o nodos de la capa fog y/o de borde, utilizando tecnologías y herramientas de disponibles y accesibles en el contexto local. Las características de esta implementación se pueden considerar un aporte a la reducción de la superficie de ataque física, aumentando la seguridad en los sistemas de IoT.

References

1. O. L. Marianetti, A. Iglesias, L. Arce. "Diseño de un prototipo de procesador soft-core para aplicaciones en nodos de WSN I '. Revista Ciencia y Tecnología, (2017). Online ISSN 2344-9217 | Print ISSN 1850-0870. Universidad de Palermo. Facultad de Ingeniería.
2. A Lattice Semiconductor White Paper. “IoT Sensor Connectivity and Processing with Ultra-Low Power, Small Form-Factor FPGAs”. (2018). https://www.latticesemi.com.
3. Argyrios Sideris, Theodora Sanida, Minas Dasygenis. “Hardware Acceleration of the AES Algorithm using Nios-II Processor”. Panhellenic Conference on Electronics & Telecommunications (PACET). (2019). DOI: 10.1109/PACET48583.2019.8956285.