Cod. 9041 | Tecnología de los ordenadores | 3304.12 Dispositivos de control

Ciberseguridad en infraestructuras. Aplicación a los elementos de un Smart Grid

Cyber security in infrastructures. Application to the components of a Smart Grid

Dionisio Ramírez[1], Valentín Ramírez[2] y Giri Venkataramanan[3]

[1] Universidad Politécnica de Madrid (España)
[2] Fábrica Nacional de Moneda y Timbre (España)
[3] WEMPEC Wisconsin-Madison University (USA)

DOI: http://dx.doi.org/10.6036/9041

Las plantas de generación, las subestaciones, etc. de una Smart Grid tienen necesidad de conectarse a Internet para comunicarse entre ellas o con centros de control. Sin embargo, las normas más utilizadas para estandarizar este tipo de comunicaciones no están bien adaptadas a esta necesidad, mientras que otras están en fase de elaboración.

En el artículo se propone una solución que aporta un alto nivel de seguridad apoyándose en los requisitos incluidos en el Esquema Nacional de Seguridad del Reino de España y que, al apoyarse exclusivamente en protocolos y criptografía estándar, resultará compatible con cualquier normativa al respecto.

1. ALCANCE DEL TRABAJO

Este trabajo muestra cómo, con una placa Gateway de precio y tamaño muy reducido, se pueden implementar medidas de seguridad fuertes como el cifrado simétrico AES 128, criptografía asimétrica RSA con claves de 2048 bits y algoritmo de hash SHA-256, adecuadas para la protección de infraestructuras conectadas a redes abiertas.

El trabajo que presentamos nació de la necesidad de conectar de forma segura los elementos de una Smart Grid a Internet. Por ello, todo el trabajo se desarrolla en este ámbito de la ingeniería. A lo largo del artículo se justifica razonadamente que la solución obtenida se integra correctamente con toda la normativa que afecta a este tipo de infraestructuras.

Finalmente, se demuestra la validez del trabajo construyendo un prototipo totalmente funcional que protege la conexión de una subestación o un elemento de una planta de generación a dichas redes abiertas y que cumple todos los requisitos del Esquema Nacional de Seguridad español.

En el punto de partida de este trabajo observamos que el estándar actualmente utilizado para las comunicaciones de los diferentes equipos (equipos de protección, control y medida) dentro de una subestación es el IEC 61850 [1, 2]. Este estándar se diseñó como solución frente a los múltiples protocolos propietarios y dispositivos de diferentes fabricantes que no es posible comunicar entre sí.

Sin embargo, aunque IEC 61850 aborda el tema de las comunicaciones, no aborda aspectos técnicos de ciberseguridad ya que se delegan a otro estándar, el IEC 62351, específicamente en la parte IEC 62351-6 [3].

Estos dos estándares son adecuados para securizar las comunicaciones dentro de una planta de generación, muchas veces un entorno controlado, pero no están específicamente diseñados para la conexión de las subestaciones a una red totalmente abierta, como Internet.

Este trabajo, por contra, propone una solución al problema de la conexión segura de infraestructuras al ciberespacio y para ello toma como referencia la Guía/Norma de seguridad de las TIC (CCN-STIC 807) "Criptología de empleo en el Esquema Nacional de Seguridad" [4], emitida por el Centro Nacional de Inteligencia español.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, le encomienda el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada. En la guía emitida por este organismo se presentan los algoritmos criptográficos que han sido acreditados para su uso en el Esquema Nacional de Seguridad.

Las recomendaciones de seguridad incluidas en este documento se basan en protocolos y algoritmos totalmente estándar por lo que será totalmente compatible con otros estándares más específicos de la industria, como la norma IEC 62443 "Seguridad para los sistemas de automatización y control industrial" [5] actualmente en fase de elaboración.

De una forma más amplia, se puede decir que, al centrarse este trabajo en el uso de criptografía estándar para la protección fuerte de las infraestructuras conectadas a redes abiertas, deberá resultar compatible con cualquier norma internacional centrada en ciberseguridad.

Otra de las preocupaciones que se aborda es el del retardo que introduce el cifrado de los datos intercambiados en las comunicaciones, que obliga a desestimar su empleo en algunas infraestructuras. En este artículo veremos que, gracias al uso de productos muy especializados), se puede reducir los tiempos de cifrado a valores insignificantes, permitiendo cumplir los 4ms de procesamiento que se recomienda IEC 62351-6 para los protocolos GOOSE y SV (Sample Values) [6].

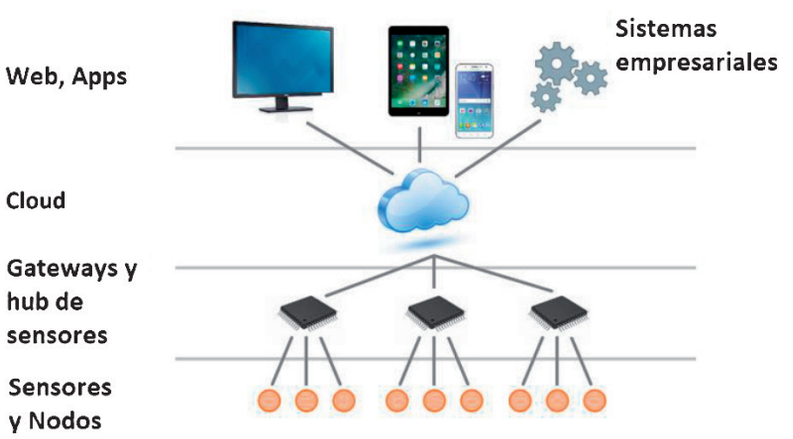

Fig.1: Arquitectura de la red de Nodos

Quedan fuera del ámbito de este trabajo, los siguientes puntos:

En este trabajo se ha supuesto que la conexión de cada elemento al Gateway es de tipo cableado, y que su seguridad se basa en los actuales estándares IEC 61850 y IEC 62351 específicos para conexiones internas en las Smart Grids.

Otras soluciones de seguridad para enviar datos a través de routers, como es el empleo de tunneling.

El formateo de los datos a intercambiar y la protección contra ataques que no se contrarresten mediante el uso de la criptografía en el Gateway, como es el Denial of Service (DoS).

La capa que codifica los datos y mensajes según IEC 61850 es totalmente estándar, común a cualquier proyecto de este tipo y, por tanto, independiente de él. Cualquier codificador comercial válido para otros proyectos es válido para éste ya que están en capas independientes. Por todo ello, y debido a lo limitado del espacio disponible en el artículo, no se ha tratado este asunto con más profundidad.

2.MATERIAL Y MÉTODOS

2.1. RED DE NODOS PROPUESTA

Las comunicaciones son un elemento clave de toda Smart Grid, ya sea entre los elementos que la componen o entre éstos y el operador que gestiona la red, al que le envían datos de generación, consumo de las cargas, etc. y del que reciben consignas de potencia, conexión, desconexión, etc. En este trabajo se ha adaptado una red basada en Nodos, para ser utilizada en una Smart Grid. A continuación, se describe dicha red y los elementos que la componen.

2.1.1. Arquitectura de la red de Nodos

La red de comunicación, Fig.1, que se propone en este trabajo se compone de Nodos (Nodos generadores y Nodos carga inteligentes, controlados todos ellos por microprocesador), de una Puerta de Enlace o Gateway para conectar los Nodos a la Nube y de los interfaces con los que el usuario interacciona con la Smart Grid mientras que la comunicación entre dispositivos o con el usuario se basa en Internet Protocol (IP).

2.1.2. Nodos

En la arquitectura propuesta, cada uno de los Nodos generadores dispone de un microcontrolador que gestiona la potencia enviada a la red mediante un convertidor de potencia conectado a la red trifásica. Igualmente, los Nodos carga disponen de capacidades de comunicación para recibir órdenes de conexión desconexión, enviar datos de consumo, interpretar tarifas horarias para optimizar el consumo, etc.

Las capacidades de los microcontroladores (MCU) utilizados en estos tipos de sistemas ha aumentado mucho en los últimos años y los más avanzados pueden ser de doble núcleo. En ellos, uno de los núcleos, con un hardware muy especializado, se encargue de las tareas de control en tiempo real mientras que el otro núcleo, con una arquitectura más convencional, se encargue de las comunicaciones.

2.1.3. Gateway seguro

La Puerta de Enlace o Gateway de una red local o de entorno controlado, funciona como el canal de comunicación entre los Nodos y el mundo exterior a través de la Nube o Cloud [7].

El Gateway seguro puede ser visto como un proveedor de seguridad para los Nodos. Este tipo de servidor puede enviar datos de forma segura a través de la conexión Ethernet y asegurarse de que solo el personal autorizado accede a dichos datos. Para ello, antes de enviar los datos, puede encriptarlos y/o firmarlos dependiendo del nivel de seguridad requerido. Los microprocesadores destinados a esta tarea se diseñan específicamente y disponen de una capacidad extra de memoria RAM y un cripto-procesador.

Para llevar a cabo la conexión de los Nodos con la Nube se seleccionó un Gateway con capacidad criptográfica. Su finalidad es que el usuario o la capa superior de control pueda acceder de manera segura a todos los Nodos a través de un único punto y desde cualquier punto que dispusiera de conexión a Internet, Fig.2. Para ello, se escogió un Tiva TM4C129ENCPDT [8, 9] del fabricante Texas Instruments, basado en una arquitectura ARM Cortex M4 y el software [10]. Este modelo dispone de un potente criptoprocesador para acelerar los cálculos criptográficos. El stack escogido fue, de nuevo, lwIP.

2.2. CONEXIÓN SEGURA

En casos de una infraestructura crítica como una Smart Grid, resulta necesario encriptar las comunicaciones para garantizar la seguridad así que este será uno de los siguientes pasos. Sin embargo, no es suficiente: también es necesario que ambos extremos de la comunicación tengan la certeza de que están comunicándose con alguien autorizado. Por tanto, resulta necesario implementar algún mecanismo de mutua autenticación entre extremos que garantice la identidad de las partes [11].

La autenticación utilizada en este trabajo se ha realizado asignando una identidad digital a cada una de las máquinas conectadas. Para ello, una Infraestructura de Clave Pública (PKI) debe encargarse de crear, gestionar, distribuir, utilizar y revocar certificados digitales asociados con la dirección IP de cada máquina, así como de encriptar la clave pública.

Para lograr esto, todas las máquinas tienen que cumplir los requisitos de identidad y confidencialidad, utilizando un protocolo de seguridad estándar como SSL o TLS para establecer un canal autenticado y cifrado. Los envíos que se hagan firmados permitirán, además, la verificación de la integridad a partir del hash del dato. Esta verificación de integridad también se puede lograr por otros medios, como añadir al final de cada envío unos bytes de checksum que se pueden obtener, por ejemplo, con un cálculo basado en el algoritmo AES y modo de operación CBC-MAC.

2.2.1. Tecnología software de seguridad

Para la securización del Gateway, Fig.3, se utilizó un sistema operativo dise-

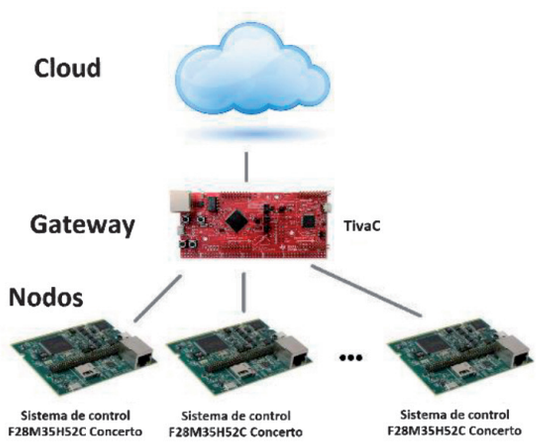

Fig. 2: Esquema de la solución escogida

ñado para sistemas embebidos denominado TI-RTOS con el fin de sacar provecho de su capacidad de multi-thread.

Como software de seguridad se seleccionó la librería criptográfica WolfSSL [12], especialmente diseñada para sistemas embebidos, y que es capaz de ofrecer conexiones TLS con las características necesarias.

Cabe destacar que la solución implementada es fácilmente migrable a otros microcontroladores Cortex M del mismo fabricante.

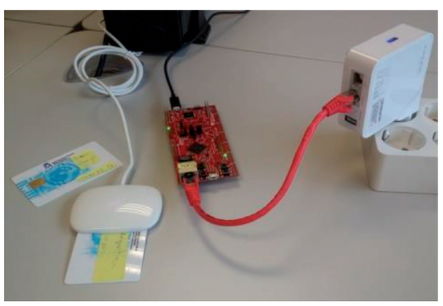

Fig. 3: Entorno de desarrollo de la solución, y pruebas de integración

2.2.1.1. Infraestructura de clave pública

La conexión TLS se basa en el uso de claves y certificados digitales que son emitidos por Infraestructuras de Clave Pública (PKI), y que permiten autenticar a personas y cosas de manera segura.

En este proyecto se crearon dos PKI, utilizando el software OpenSSL [13].

- PKI para la emisión de certificados de Servidor.
- PKI para la emisión de certificados de Cliente.

Los certificados de Servidor y sus claves privadas correspondientes están destinados a posibilitar que cualquier cliente que se conecte al servidor, pueda validar la identidad del mismo, evitando así ataques basados en la suplantación del servidor.

Los certificados de Cliente y sus claves privadas correspondientes están destinados a que el servidor seguro pueda verificar la identidad de aquellas entidades (personas u otras máquinas) que se conecten a él, para verificar si están autorizadas a conectarse a él y recibir la información.

2.2.1.2. Almacenamiento de claves y certificados

El proyecto se desarrolló para soportar tres posibilidades:

- Almacenamiento de claves criptográficas y certificados en el computador, mediante los navegadores Web instalados en la máquina.
- Almacenamiento de claves criptográficas y certificados en tarjetas inteligentes criptográficas de tipo Dual Interface, Fig.4 que pueden ser usadas en los navegadores web de los ordenadores personales mediante un lector de tarjetas convencional, o en dispositivos móviles, mediante la antena NFC que ya está disponible en la mayoría de estos dispositivos.
- Almacenamiento de claves criptográficas y certificados en el código fuente de aplicaciones (App) destinadas a su uso en dispositivos móviles con sistema operativo Android.

Fig. 4: a) Tarjeta criptográfica proporcionada por la FNMT-RCM y lector utilizado en el ordenador cliente. b) Petición de la clave de acceso a la tarjeta inteligente utilizada

La Fig.5 muestra las propiedades de la conexión segura, una vez establecida entre el Gateway y el PC utilizando el protocolo TLS v1.2. En la descripción mostrada por el navegador Chrome aparecen las características siguientes: el parámetro ECDHE y P-256 indican que se ha utilizado criptografía asimétrica de curvas elípticas para realizar el intercambio de claves Diffie-Hellman, y que se ha utilizado la curva P-256, predefinida por el Institute of Standards and Technology (NIST) de EE. UU. El parámetro RSA indica que se ha utilizado autenticación mutua basada en criptografía asimétrica de 2048 bits y que su validez ha sido verificada.

El parámetro AES_128_GCM indica que el intercambio de datos se ha realizado utilizando criptografía simétrica basada en el algoritmo AES con clave de 128 bits y modo GCM.

Con todas estas características, se puede decir que la comunicación presenta un grado de protección muy elevado.

3. RESULTADOS

El resultado del proyecto ha sido un sistema real de laboratorio que representa un Nodo formado por un generador basado en energía renovable, incluyendo convertidores electrónicos y máquina, conectado de forma segura a la Nube a través de un Gateway con capacidad criptográfica.

Los niveles de seguridad implementados han sido dos: encriptación e identidad digital.

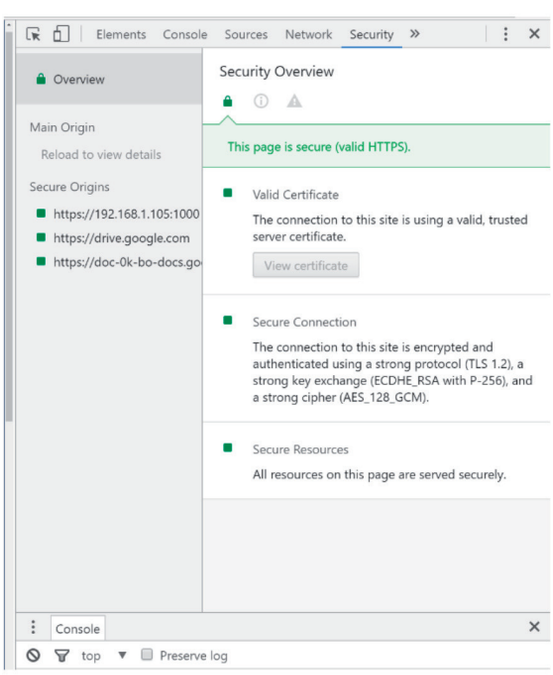

Fig. 5: En margen derecho de la ventana del navegador Crome se pueden comprobar las propiedades de la criptografía utilizada en la conexión

Como resultado fue posible establecer una conexión con el Nodo a través del Gateway y monitorizar sus variables (tensiones y corrientes del generador, por ejemplo) o enviarle comandos de control, y todo ello de forma segura.

La capa de seguridad utilizada limita el acceso a los Nodos a las personas autorizadas, que deben poseer el certificado digital adecuado, ya sea en una tarjeta o instalado en su ordenador. Además, la encriptación fuerte utilizada hace improbable el hackeo de la comunicación sin por ello interferir apreciablemente en el flujo de datos.

4. DISCUSIÓN

4.1. FORTALEZAS DE LA ARQUITECTURA DE SEGURIDAD ESCOGIDA

La principal fortaleza de la solución adoptada es la flexibilidad a la hora de configurar clientes con un nivel de seguridad adaptado a las necesidades de cada proyecto.

Tan sólo es necesario cargar el certificado de la CA raíz que emite los certificados del Cliente, para poder ser empleados para autenticarse frente al servidor seguro.

Se han probado soluciones en las que la clave privada y el certificado de Cliente estaban almacenados de diferentes formas, y por tanto con diferentes niveles de seguridad

- Clave privada y certificado de Cliente almacenado en el navegador web (Edge, Explorer, Firefox).
- Clave privada y certificado de Cliente almacenado en una tarjeta criptográfica, a la cual accede el navegador web (Edge, Explorer, Firefox) para autenticarse frente al servidor.
- Clave privada y certificado de Cliente almacenado en aplicación Android.
- Clave privada y certificado de Cliente almacenado en una tarjeta criptográfica, a la cual accede la App Android para autenticarse frente al servidor.

Las diferencias observadas entre las diferentes formas de almacenamiento propuestas son:

- El almacenamiento en el computador aporta facilidad de uso, ya que los navegadores Web son capaces de manejarlos directamente, y no es necesario presentar ninguna clave de acceso (PIN) para poder usarlos. Por contra, es menos seguro que otros métodos, ya que su nivel depende del grado de "bastionamiento" del equipo informático en el que se almacenan.
- El almacenamiento en tarjeta inteligente criptográfica aporta el mayor nivel de seguridad, ya que los chips empleados en ellas están especialmente enfocados a la seguridad, y pasan estrictos procesos de certificación de su seguridad.
- El almacenamiento en aplicaciones específicas para dispositivos móviles tiene como ventaja el ofrecer el mayor nivel de usabilidad. Sin embargo, su seguridad se ve muy condicionada por las características del hardware, en particular, de si dispone de un secure element (elemento seguro) interno, donde almacenar las claves.
- En el caso de los dispositivos móviles, las aplicaciones pueden hacer uso de las capacidades criptográficas de las tarjetas inteligentes dual interface, accediendo a ellas a través de su antena NFC. Esta forma de trabajar es muy segura, ya que el chip de la tarjeta actúa como secure element (elemento seguro) del móvil, pudiéndose aprovechar éste del potente criptoprocesador incluido en el chip del a tarjeta para llevar a cabo operaciones de criptografía asimétrica, tanto para autenticación, como para firma digital.

4.2. DEBILIDADES DE LA ARQUITECTURA DE SEGURIDAD ESCOGIDA

Desde el punto de vista de la seguridad, los dos principales inconvenientes de la solución adoptada son:

- La clave privada de autenticación del servidor está almacenada en la memoria Flash convencional del microcontrolador ARM Cortex M4, es decir, en una memoria de almacenamiento "en claro", no encriptada.
- La clave privada de autenticación del servidor está hardcoded en el código fuente del servidor y es por tanto la misma para todos nuestros servidores.

4.3. ADAPTACIÓN A USO EN REDES INTERNAS

Como ya se ha comentado, el estándar actualmente utilizada en comunicaciones de equipos de protección, control y medida es el definido en la norma IEC 61850 [1, 2]. En ella se definen los eventos genéricos de subestación (GSE) diseñados para comunicar eventos genéricos de la subestación a varios dispositivos electrónicos inteligentes dentro del sistema, de manera simultánea, rápida y segura. Los GSE son un modelo de control definido según EN 61850 "Sistemas y redes de comunicación para la automatización de las redes de potencia de las compañías eléctricas" que proporciona un mecanismo para transferir datos de eventos a través de redes de subestaciones eléctricas. Sin embargo, no aborda aspectos técnicos de ciberseguridad, ya que se delegan a otro estándar, el definido en la IEC 62351, Power systems management and associated information exchange – Data and communications security –Part 6: Security for IEC 61850 [3] que especifica mensajes, procedimientos y algoritmos para securizar los protocolos basados en la norma IEC 61850.

El modelo de control definido en EN 61850 [1, 2] busca garantizar que el mismo mensaje de evento sea recibido por múltiples dispositivos físicos utilizando servicios de difusión múltiple o multidifusión. El modelo de control GSE se subdivide en GOOSE (eventos genéricos de subestación orientados a objetos) y GSSE (eventos genéricos de estado de subestaciones).

Aunque queda fuera del ámbito de este proyecto el intercambio de mensajes basado en GOOSE, se estima que el trabajo presentado en este artículo se podría adaptar de una forma sencilla a este uso aportando, además, valor a la infraestructura.

En aquellas aplicaciones que utilizan IEC 61850-9-2 y GOOSE que requieran un tiempo de respuesta inferior a 4 milisegundos, con configuraciones de multidifusión y de bajo consumo de CPU, la Technical Specification TS 62351 en su apartado 6 [3] recomienda no emplear el cifrado de datos. En su lugar, recomienda utilizar un proceso de selección de ruta de comunicación para garantizar la confidencialidad de los intercambios de información.

En relación con estas limitaciones, y atendiendo a las características que ofrece el microcontrolador del Gateway seleccionado para este proyecto, podemos decir que:

Microcontroladores como el Tiva™ TM4C129ENCPDT [8] incluyen un potente acelerador criptográfico hardware. Esto le permite obtener fantásticos tiempos de ejecución en las operaciones de cifrado de datos y de hash:

- En operaciones de cifrado con algoritmo AES y claves de 192 bits se emplean 0.3 microsegundos para cifrar 16 bytes.

- En operaciones con el algoritmo de resumen SHA-256, se emplea un tiemplo máximo de 0,54 microsegundos por cada bloque de 64 bytes.

También, dado que la estructura de los mensajes intercambiados mediante GOO-

SE tienen una parte fija, de unos pocos bytes de longitud, y una sección VARIABLE que incluye los campos TAG, LONGITUD, VALOR, dependiendo del tamaño máximo de los mensajes intercambiados, será posible plantearse el uso de cifrado de datos en aplicaciones con requisito de tiempos de respuesta inferiores a 4ms, como GOOSE, manteniendo el cifrado de los datos.

5. CONCLUSIONES

El principal valor de este trabajo se centra el utilizar un pequeño Gateway del fabricante Texas Instruments, para logar una solución robusta (basada en criptografía fuerte), sencilla y barata, que permita securizar la conexión de una infraestructura a una red abierta, como Internet. Específicamente, el trabajo ha demostrado su validez en la conexión de los elementos de una Smart Grid a redes abiertas cumpliendo, además, los requisitos del Esquema Nacional de Seguridad español.

Sobre un prototipo de laboratorio que representa un Nodo formado por un generador basado en energía renovable (ver en material suplementario), en el que se han utilizado microcontroladores específicos con stacks TCP/IP adaptados y haciendo uso de un Gateway con capacidad criptográfica, ha sido posible implementar un sistema de comunicación a través de Internet para comunicarle de manera segura con el resto de los Nodos de una red y con la Nube.

La tecnología de seguridad aplicada en este prototipo ha permitido conectar a través de Internet todos los elementos de la red de una forma sencilla y segura. Esto representa una ventaja substancial y significativa para facilitar la generalización de la interconexión confiable y sin riesgos de los elementos de una Smart Grid.

La utilización de criptografía fuerte para proteger los dispositivos no ha supuesto un retraso importante en el manejo de datos por parte de los sistemas de monitorización y control conectados a los Nodos.

La tecnología utilizada hace posible una conexión sencilla y segura del Gateway (y, por tanto, de los Nodos) a dispositivos portátiles como smartphones y tablets conectados a la Nube para realizar una monitorización remota.

Finalmente, gracias a la flexibilidad y compatibilidad de la tecnología utilizada, ha sido posible realizar interfaces de usuario utilizando los softwares más conocidos: LabVIEW, Matlab, HTML, etc.

Este trabajo muestra cómo, con una pequeña inversión en ingeniería, es posible dotar a cada uno de los elementos de una infraestructura crítica como es una Smart Grid, de los más altos niveles de seguridad, utilizando los más modernos protocolos, los algoritmos más avanzados y las longitudes de clave recomendadas por las agencias de seguridad.

En la Guía/Norma de seguridad de las TIC CCN-STIC 807, "Criptología de empleo en el Esquema Nacional de Seguridad" se explica que el uso del algoritmo RSA implicará tamaños de clave cada vez mayores. Por ello, una posible evolución futura sería migrar el prototipo hacia el uso de criptografía asimétrica basado en el algoritmo de Curvas Elípticas con claves de 256 bits, cuya fortaleza es aproximadamente equivalente a la que aporta el algoritmo RSA con claves de 3072 bits. La evolución nos permitiría emplear tamaños de clave significativamente menores, una carga de procesamiento muy inferior y, por tanto, obtener unos tiempos de ejecución muy mejorados.

La tecnología de Internet de las Cosas (IoT) dispone de protocolos desarrollados específicamente para conectar sistemas con topología en estrella y un gran número de nodos, lo que parece encajar con la problemática de una red como la empleada en este trabajo, por lo que podría ser interesante estudiar su idoneidad. El protocolo de IOT más conocido es MQTT (Message Queue Telemetry Transport), un protocolo diseñado específicamente para la conectividad Machine-to-Machine (M2M), que admite autenticación mediante certificados digitales y canal seguro TLS/SSL. Está enfocado al envío de datos en aplicaciones donde se requiere muy poco ancho de banda. Además, sus características hacen que tenga un consumo realmente bajo y precisa de muy pocos recursos para su funcionamiento. Sigue una topología en estrella, donde existe un nodo central o broker con capacidad para trabajar con un gran número de clientes. Emplea una comunicación en la que emisores y receptores deben estar subscritos a un topic común para poder entablar la comunicación.

En la organización interna de la red de nodos de este trabajo no se ha empleado MQTT porque el objeto de este trabajo no era explorar nuevas arquitecturas de redes internas, sino la conexión segura de un elemento de una planta de generación a una red abierta. Sin embargo, podría ser un tema interesante para desarrollar un futuro trabajo y un artículo explicando las ventajas e inconvenientes de uso en Smart Grids. Modificar el software del Gateway para utilizarlo en una arquitectura MQTT sería una tarea trivial, lo que ya es un buen punto de partida.

REFERENCIAS

[1] La ciberseguridad en las subestaciones y el estándar IEC 61850. https://www.incibe-cert.es/en/blog/substation-cybersecurity-iec61850-standard.
[2] EN 61850-6:2010 Communication networks and systems for power utility automation - Part 6: Configuration description language for communication in power utility automation systems related to IEDs (IEC 61850-6:2009/A1:2018).
[3] TECHNICAL SPECIFICATION IEC TS 62351-6 Power systems management and associated information exchange – Data and communications security –Part 6: Security for IEC 61850.
[4] Guía/Norma de seguridad de las TIC (CCN-STIC 807) "Criptología de empleo en el Esquema Nacional de Seguridad".
[5] UNE-EN IEC 62443-4-1:2018. Seguridad para los sistemas de automatización y control industrial.
[6] Cybersecurity for shared infrastructure substation networks with IEC 61850 GOOSE and Sampled Values. https://digital-library.theiet.org/content/journals/10.1049/joe.2018.0150
[7] Joe Folkens. Building a gateway to the Internet of Things. Texas Instruments. December 2014.
[8] Tiva TM4C129ENCPDT Microcontroller. DATA SHEET. 2014. Texas Instruments Incorporated. DS-TM4C129ENCPDT-15863.2743.
[9] ARM Cortex-M4F-Based MCU TM4C129E Crypto Connected LaunchPad for IoT Applications. http://www.ti.com/tool/EK-TM4C129EXL
[10] TivaWare™ for C Series (Complete). http://www.ti.com/tool/SW-TM4C
[11] Overview of Authentication and Authorization Technologies and Solution End. States https://technet.microsoft.com/en-us/library/bb463152.aspx?f=255&tMSPPError=-2147217396
[12] WolfSSL Texas Instruments Support. https://www.wolfssl.com/docs/ti/
[13] OpenSSL. Cryptography and SSL/TLS Toolkit. https://www.openssl.org/

AGRADECIMENTOS

Los autores desean mostrar su agradecimiento a la FNMT-RCM por aportar las tarjetas criptográficas y actuar como la necesaria Infraestructura de Clave Pública, así como por su colaboración y apoyo en el desarrollo de la infraestructura de seguridad; a WolfSSL por el apoyo desinteresado con la librería SSL para sistemas embebidos; a ST microelectronics y Texas Instruments University Europe por su aportación desinteresada del hardware utilizado y de su conocimiento técnico.
Este trabajo se enmarca en el proyecto DPI2017-88505-C2-1-R de la convocatoria de proyectos de I+D+i, del Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad.

MATERIAL SUPLEMENTARIO

http://www.revistadyna.com/documentos/pdfs/_adic/9041-1.pdf